Cours d'arithmétique

Première partie

Pierre Bornsztein
Xavier Caruso
Pierre Nolin
Mehdi Tibouchi

Décembre 2004

Ce document est la première partie d'un cours d'arithmétique écrit pour les élèves préparant les olympiades internationales de mathématiques. Le plan complet de ce cours est :

1. Premiers concepts
2. Division euclidienne et conséquences
3. Congruences
4. Équations diophantiennes
5. Structure de $\mathbf{Z}/n\mathbf{Z}$
6. Sommes de carrés
7. Polynômes à coefficients entiers
8. Fractions continues

Cette première partie traite les quatre premiers chapitres. Les quatre derniers chapitres forment quant à eux la deuxième partie de ce cours.

Contrairement à la seconde partie, cette première partie se veut le plus élémentaire possible. Les notions abstraites, souvent plus difficiles à assimiler, mais qui clarifient les idées lorsqu'elles sont comprises, ne sont évoquées que dans la seconde partie. Nous conseillons au lecteur de bien maîtriser ce premier tome avant de passer à la lecture du second.

Les notions et les théorèmes introduits ici sont généralement tout à fait suffisants pour traiter les exercices proposées aux olympiades internationales de mathématiques.

Vous trouverez à la fin de chaque chapitre une série d'exercices de difficulté variable mais indiquée par des étoiles[1]. Toutes les solutions sont rassemblées à la fin du document.

Nous vous souhaitons bon apprentissage et bonne lecture.

[1] Plus nous avons jugé l'exercice difficile, plus le nombre d'étoiles est important.

Liste des abbrévations :

AMM	American Mathematical Monthly
APMO	The Asian Pacific Mathematics Olympiad
CG	Concours général
OIM	Olympiades Internationales de Mathématiques
SL	Short List
TDV	Tournoi Des Villes

Liste des notations :

$\varnothing$	ensemble vide
$\mathbf{N}$	ensemble des entiers naturels (positifs ou nuls)
$\mathbf{N}^\star$	ensemble des entiers naturels strictement positifs
$\mathbf{Z}$	ensemble des entiers relatifs
$\mathbf{Q}$	ensemble des nombres rationnels
$\mathbf{R}$	ensemble des nombres réels
$\sum$	symbôle de sommation[2]
$\prod$	symbôle de produit[3]
$a \mid b$	a divise b
$[x]$	partie entière de x
$\{x\}$	partie décimale de x
PGCD	plus grand commun diviseur
$a \wedge b$	PGCD (a, b)
PPCM	plus petit commun multiple
$a \vee b$	PPCM (a, b)
$a \equiv b \pmod N$	a est congru à b modulo N
p	un nombre premier
$v_p(n)$	valuation p-adique de n
$d(n)$	nombre de diviseurs positifs de n
$\sigma(n)$	somme des diviseurs positifs de n
φ	fonction indicatrice d'Euler
$s_b(n)$	somme des chiffres de n en base b
$\pi(n)$	nombre de nombres premiers inférieurs ou égaux à n
$\overline{a_n \dots a_0}^b$	écriture en base b
$n!$	factorielle de n : $n! = 1 \times 2 \times \cdots \times n$
C_n^k	coefficient binomial : $\mathrm{C}_n^k = \frac{n!}{k!(n-k)!}$
$u_n \sim v_n$	les suites (u_n) et (v_n) sont équivalentes

[2]Une somme indexée par l'ensemble vide est égale à 0.
[3]Un produit indexé par l'ensemble vide est égale à 1.

Table des matières

1 Premiers concepts

Cette section, comme son nom l'indique, présente le concept de base de l'arithmétique, à savoir la divisibilité. On introduit ensuite les nombres premiers ce qui permet d'énoncer le théorème fondamental de l'arithmétique (c'est-à-dire la décomposition en facteurs premiers) dans lequel les nombres premiers jouent le rôle de briques élémentaires pour la fabrication des nombres.

1.1 Divisibilité

Définition 1.1.1 Si a et b sont deux entiers, on dit que a *divise* b, ou que b est *divisible* par a, s'il existe un entier q tel que $b = aq$. On dit encore que a est un *diviseur* de b, ou que b est un *multiple* de a. On le note $a|b$.

Propriétés

- ☞ Si a et b sont deux entiers avec $b \neq 0$, b divise a si et seulement si la fraction $\frac{a}{b}$ est un entier.
- ☞ Tous les entiers divisent 0, et sont divisibles par 1.
- ☞ Un entier n est toujours divisible par 1, -1, n et $-n$.
- ☞ Si $a|b$, et $b|c$, alors $a|c$.
- ☞ Si $a|b_1, b_2, \ldots, b_n$, alors $a|b_1c_1+b_2c_2+\ldots+b_nc_n$, quels que soient les entiers $c_1, c_2, \ldots, c_n$.
- ☞ Si a divise b et $b \neq 0$, alors $|a| \leqslant |b|$.
- ☞ Si a divise b et b divise a, alors $a = \pm b$.
- ☞ Si a et b sont deux entiers tels que $a^n|b^n$ pour un entier $n \geqslant 1$, alors $a|b$.

Toutes les propriétés listées précédemment sont immédiates, à l'exception de la dernière dont la démonstration n'est pas triviale sans bagage arithmétique. Une preuve possible consiste à utiliser la caractérisation de la divisibilité par les valuations p-adiques (voir paragraphe 1.3).

Voyons immédiatement deux exercices qui montrent comment on peut manipuler la notion de divisibilité :

Exercice : Soient x et y des entiers. Montrer que $2x + 3y$ est divisible par 7 si et seulement si $5x + 4y$ l'est.

Solution : Supposons que 7 divise $2x + 3y$, alors il divise $6(2x + 3y) - 7(x + 2y) = 5x + 4y$. Réciproquement si 7 divise $5x + 4y$, il divise $6(5x + 4y) - 7(4x + 3y) = 2x + 3y$. √

Exercice : Pour quels entiers n strictement positifs, le nombre $n^2 + 1$ divise-t-il $n + 1$?

Solution : Si $n^2 + 1$ divise $n + 1$, comme tout est positif, on doit avoir $n^2 + 1 \leqslant n + 1$, ce qui n'est vérifié que pour $n = 1$. On vérifie ensuite que $n = 1$ est bien solution. √

Parties entières

Définition 1.1.2 Si x est un réel, on appelle *partie entière* de x, et on note $[x]$, le plus grand entier inférieur ou égal à x. Ainsi, on a $[x] \leqslant x < [x] + 1$.

Remarque. On définit aussi la *partie décimale* de x, comme la différence $x - [x]$. La partie décimale de x est souvent notée $\{x\}$. Cette notion est moins utilisée que la notion de partie entière et les conventions de notations sont moins usuelles à ce propos : lors d'un exercice, ou d'un exposé, il est toujours de bon goût de commencer par préciser les notations qui vont être employées par la suite.

Notons qu'il faut être prudent avec les nombres négatifs : autant pour les nombres positifs, la partie entière correspond au nombre auquel on retire ses chiffres après la virgule, autant ce n'est pas le cas pour les nombres négatifs. En effet, si on suit la définition, on voit par exemple que $[-3,5] = -4$.

Les parties entières et parties décimales obéissent à quelques propriétés élémentaires que nous listons ci-dessous :

Propriétés élémentaires

☞ On a toujours $x = [x] + \{x\}$.

☞ Pour tout réel x, on a $x - 1 < [x] \leqslant x$

☞ Si x est entier, $[x] = x$ et $\{x\} = 0$. Et réciproquement si l'une des deux égalités est vérifiée, alors x est entier.

☞ $[-x] = -[x] - 1$ sauf si x est entier, auquel cas $[-x] = -[x]$.

☞ Si x et y sont deux réels, $[x] + [y] \leqslant [x + y] \leqslant [x] + [y] + 1$.

☞ Si $m > 0$ est un entier, alors il y a exactement $[\frac{x}{m}]$ multiples de m compris entre 1 et x.

La démonstration des propriétés consiste en de simples manipulations de la définition et principalement de l'inégalité $[x] \leqslant x < [x] + 1$. Elle est laissée au lecteur. On remarquera que très souvent les questions faisant intervenir des parties entières se résument à de la manipulation d'inégalités comme le montre par exemple l'exercice suivant :

<u>*Exercice*</u> : On suppose que $4n + 2$ n'est pas le carré d'un nombre entier. Montrer que pour $n \geqslant 0$, on a :

$$\left[\sqrt{n} + \sqrt{n+1}\right] = \left[\sqrt{4n+2}\right]$$

<u>*Solution*</u> : Remarquons tout d'abord que l'on a toujours l'inégalité :

$$\sqrt{n} + \sqrt{n+1} < \sqrt{4n+2}$$

En effet, en élevant au carré, on a à comparer $2n + 1 + 2\sqrt{n^2 + n}$ et $4n + 2$, soit $2\sqrt{n^2 + n}$ et $2n + 1$ et l'inégalité devient évidente après une nouvelle élévation au carré.

Il reste à prouver qu'il n'existe aucun entier k tel que :

$$\sqrt{n} + \sqrt{n+1} < k \leqslant \sqrt{4n+2}$$

soit, encore en élevant au carré qu'il n'existe aucun entier k tel que :

$$2n + 1 + 2\sqrt{n^2 + n} < k^2 \leqslant 4n + 2$$

Mais il est clair que $4n + 1 < 2n + 1 + 2\sqrt{n^2 + n}$ et un tel entier k vérifirait *a fortiori* $4n + 1 < k^2 \leqslant 4n + 2$. Comme k est entier, il vient forcément $k^2 = 4n + 2$, mais cela n'est pas possible puisque l'on a supposé que $4n + 2$ n'était pas le carré d'un entier. $\surd$

Remarque. En fait, $4n + 2$ n'est jamais le carré d'un entier. En effet, le nombre $4n + 2$ est pair, et s'il était le carré d'un entier, il serait le carré d'un entier pair. Mais alors $4n + 2$ devrait être un multiple de 4, ce qui n'est, à l'évidence, pas le cas. L'égalité précédente de parties entières est donc valable pour tout entier $n \geqslant 1$, sans hypothèse supplémentaire.

Une propriété amusante des parties entières qui montre également que parfois (souvent) les manipulations d'inégalités ne sont pas faciles est le théorème de Beatty que voici :

Théorème 1.1.3 (Beatty) *Soient α et β deux réels strictements positifs. On note S_α (resp. S_β) l'ensemble des entiers strictement positifs qui s'écrivent sous la forme $[n\alpha]$ (resp. $[n\beta]$) pour un certain entier n.*

Les ensembles S_α et S_β forment une partition de $\mathbf{N}^\star$ si, et seulement si α et β sont irrationnels et vérifient $\frac{1}{\alpha} + \frac{1}{\beta} = 1$.

Démonstration. Commençons par supposer que α et β sont des irrationnels vérifiant $\frac{1}{\alpha} + \frac{1}{\beta} = 1$. Soit k un entier strictement positif. Il est dans l'ensemble S_α si et seulement s'il existe un entier n tel que :

$$n\alpha - 1 < k < n\alpha$$

l'inégalité de droite étant stricte car α est supposé irrationnel. L'équation se transforme et donne :

$$\frac{k}{\alpha} < n < \frac{k}{\alpha} + \frac{1}{\alpha}$$

Autrement dit, $k \in S_\alpha$ si et seulement si l'intervalle $\left]\frac{k}{\alpha}, \frac{k}{\alpha} + \frac{1}{\alpha}\right[$ contient un entier. De même $k \in S_\beta$ si et seulement si l'intervalle $\left]\frac{k}{\beta}, \frac{k}{\beta} + \frac{1}{\beta}\right[$ contient un entier.

L'intervalle $\left]\frac{k}{\alpha}, \frac{k}{\alpha} + 1\right[$ est de longueur 1 et ses bornes sont irrationnelles, donc il contient un et un seul entier n. Si $n < \frac{k}{\alpha} + \frac{1}{\alpha}$, alors $k \in S_\alpha$. Sinon, on a l'inégalité :

$$\frac{k}{\alpha} + \frac{1}{\alpha} < n < \frac{k}{\alpha} + 1$$

l'inégalité de gauche étant stricte car $\frac{k+1}{\alpha}$ est irrationnel et donc ne peut être égal à n. Comme $\frac{k}{\alpha} = k - \frac{k}{\beta}$, il vient :

$$\frac{k}{\beta} < k + 1 - n < \frac{k}{\beta} + \frac{1}{\beta}$$

et donc $k \in S_\beta$. Si k était à la fois élément de S_α et de S_β, il y aurait un entier dans l'intervalle $\left]\frac{k}{\alpha}, \frac{k}{\alpha} + \frac{1}{\alpha}\right[$ et un dans l'intervalle $\left]\frac{k}{\beta}, \frac{k}{\beta} + \frac{1}{\beta}\right[$ et donc par le même raisonnement que précédemment, il y en aurait deux dans l'intervalle $\left]\frac{k}{\alpha}, \frac{k}{\alpha} + 1\right[$, ce qui n'est pas possible.

Réciproquement, supposons que S_α et S_β forment une partition de $\mathbf{N}^\star$. Considérons un entier k strictement positif. Il y a $\left[\frac{k}{\alpha}\right]$ entiers dans $\{1,\dots,k\}$ qui sont dans S_α. De même, il y a $\left[\frac{k}{\beta}\right]$ entiers dans $\{1,\dots,k\}$ qui sont dans S_β. Du fait de la partition, il vient :

$$\left[\frac{k}{\alpha}\right]+\left[\frac{k}{\beta}\right]=k$$

pour tout k. En faisant tendre k vers l'infini, il vient :

$$\frac{1}{\alpha}+\frac{1}{\beta}=1$$

ce qui démontre la deuxième condition.

Supposons maintenant par l'absurde que α soit rationnel. Alors il en est de même de β d'après la relation précédente. Écrivons $\alpha=\frac{a}{b}$ et $\beta=\frac{c}{d}$. L'entier ac est élément de S_α (en prenant $n=bc$) et également élément de S_β (en prenant $n=ad$), ce qui est contradictoire. □

PGCD et PPCM

Ce paragraphe introduit les définitions de PGCD et PPCM qui sont deux notions fondamentales de l'arithmétique et en donne leurs principales propriétés. Les démonstrations qui ne sont pas évidentes sont reportées au chapitre 2 et seront vues comme conséquence de la division euclidienne.

Définition 1.1.4 Soient a et b deux entiers non tous deux nuls. L'ensemble des diviseurs communs de a et de b est fini et non vide, il possède donc un plus grand élément appelé *plus grand commun diviseur* (PGCD) de a et b et noté $\text{PGCD}\,(a,b)$.

Lorsque $\text{PGCD}\,(a,b)=1$, on dit que a et b sont *premiers entre eux*.

De même a et b possèdent un plus petit multiple commun positif, on l'appelle le *plus petit commun multiple* (PPCM) de a et de b et on le note $\text{PPCM}\,(a,b)$.

Propriétés

☞ Si $d=\text{PGCD}\,(a,b)$, alors n divise a et b si et seulement si n divise d.

☞ Si $m=\text{PPCM}\,(a,b)$, alors n est un multiple a et de b si et seulement si n est un multiple de m.

☞ Si a, b et n sont des entiers non nuls et $n>0$, alors $\text{PGCD}\,(na,nb)=n\text{PGCD}\,(a,b)$. Si de plus n divise a et b, alors $\text{PGCD}\left(\frac{a}{n},\frac{b}{n}\right)=\frac{1}{n}\text{PGCD}\,(a,b)$.

☞ Si $d=\text{PGCD}\,(a,b)$, on peut écrire $a=da'$ et $b=db'$ pour a' et b' des nombres premiers entre eux.

☞ Si a et b sont des entiers, l'égalité $\text{PGCD}\,(a,b)=\text{PGCD}\,(a,a+b)$ est toujours vérifiée lorsqu'elle a un sens. En particulier, le PGCD de deux nombres consécutifs est 1, et plus généralement, le PGCD de a et de $a+n$ est un diviseur positif de n.

☞ Plus généralement, si x, y, a, b, a' et b' sont des entiers alors :

$$\text{PGCD}\,(x,y)\mid\text{PGCD}\,(ax+by,a'x+b'y)\mid(ab'-ba')\,\text{PGCD}\,(x,y)$$

En particulier si $|ab'-ba'|=1$, alors $\text{PGCD}\,(x,y)=\text{PGCD}\,(ax+by,a'x+b'y)$.

Ces propriétés sont élémentaires. Souvent, pour prouver l'égalité de deux PGCD, on montre que chacun des PGCD divise l'autre. C'est la méthode que l'on utilise majoritairement ici. Expliquons comment on procède pour montrer qu'un PGCD en divise un autre en donnant un preuve de la dernière propriété qui est la plus difficile : notons $d = \text{PGCD}(x, y)$. Alors d divise x et y et donc il divise $ax + by$ et $a'x + b'y$ puis leur PGCD. De même, soit $d' = \text{PGCD}(ax + by, a'x + b'y)$, alors d' divise $b'(ax + by) - b(a'x + b'y) = (ab' - ba')x$ et $a'(ax + by) - a(a'x + b'y) = (a'b - b'a)y$. Ainsi d' divise $\text{PGCD}((ab' - ba')x, (a'b - b'a)y) = |ab' - ba'| \text{PGCD}(x, y)$, ce qui conclut.

Citons également des résultats classiques et souvent assez utiles :

Propriétés

- ☞ Si a et b sont des entiers non nuls alors $\text{PGCD}(a^n, b^n) = \text{PGCD}(a, b)^n$ pour tout entier $n \geqslant 0$.
- ☞ Si a, b et c sont des entiers non nuls, on a :

$$\begin{aligned}
\text{PGCD}(a, \text{PPCM}(b, c)) &= \text{PPCM}(\text{PGCD}(a, b), \text{PGCD}(a, c)) \\
\text{PPCM}(a, \text{PGCD}(b, c)) &= \text{PGCD}(\text{PPCM}(a, b), \text{PPCM}(a, c))
\end{aligned}$$

- ☞ *Théorème de Bézout.* Si a et b sont des entiers premiers entre eux, alors il existe des entiers u et v tels que $au + bv = 1$.
- ☞ *Lemme de Gauss.* Si des entiers a, b et c sont tels que a divise bc et a premier avec b, alors a divise c.
- ☞ Si deux entiers premiers entre eux a et b divisent n, alors le produit ab divise également n.

Ces propriétés sont plus difficiles. Les deux premières résultent par exemple directement de l'expression de $\text{PGCD}(a, b)$ en fonction de la décomposition en facteurs premiers de a et de b (voir la partie sur *le théorème fondamental de l'arithmétique* dans le paragraphe 1.2). Les autres résultent des propriétés de la division euclidienne que nous étudions au chapitre 2. Leur démonstration est donc reportée aux paragraphes 2.3 et 2.4.

Donnons à présent deux exercices qui montrent comment l'on peut manipuler les faits précédents :

Exercice : On définit le n-ième *nombre de Fermat* par la formule $F_n = 2^{2^n} + 1$. Montrer que les F_n sont deux à deux premiers entre eux.

Solution : On remarque que :

$$\begin{aligned}
F_{n+1} - 2 = 2^{2^{n+1}} - 1 &= \left(2^{2^n} - 1\right)\left(2^{2^n} + 1\right) \\
&= \left(2^{2^{n-1}} - 1\right)\left(2^{2^{n-1}} + 1\right)\left(2^{2^n} + 1\right) = F_n F_{n-1} \cdots F_0
\end{aligned}$$

Soit d un diviseur commun de F_n et F_m. Supposons par exemple $n < m$. D'après la formule précédente, comme d divise F_n, il divise $F_m - 2$ et donc 2. Les F_n sont clairement impairs, la seule solution est d'avoir $|d| = 1$. Ceci prouve que F_n et F_m sont premiers entre eux. $\surd$

Exercice : Soient a et b des nombres premiers entre eux. Montrer que ab et $a+b$ sont aussi premiers entre eux.

Solution : Soit d un diviseur commun de ab et de $a+b$. Alors d divise $a(a+b)-ab = a^2$. De même d divise b^2. D'après une des propriétés précédentes, les entiers a^2 et b^2 sont premiers entre eux. Ainsi $d = \pm 1$, ce qui conclut. $\surd$

1.2 Nombres premiers

Définition et exemples

Comme nous l'avons dit dans l'introduction de cette partie, les nombres premiers sont les briques élémentaires pour fabriquer les nombres. De façon plus précise et moins imagée, on a la définition suivante :

Définition 1.2.1 Un entier $n > 0$ est dit *premier* s'il est différent de 1 et s'il n'admet aucun diviseur positif différent de 1 et n. Un tel diviseur est appelé *diviseur strict.*

Un nombre qui n'est pas premier est appelé *nombre composé.*

Par définition, donc, 1 n'est pas premier. C'est une simple convention mais elle s'avère utile pour l'énoncé des théorèmes comme vous allez (peut-être) vous en rendre compte. Les entiers $2, 3, 5, 7, 11, 13$ sont les premiers nombres premiers. Le nombre 6, n'est par contre pas premier car on peut écrire $6 = 2 \times 3$ (et donc 2 (ou 3) est un diviseur strict de 6).

Proposition 1.2.2 *Soit $n > 1$ un entier. Son plus petit diviseur $d > 1$ est un nombre premier. Si de plus n est composé, alors $d \leqslant \sqrt{n}$.*

Démonstration. Supposons que d ne soit pas premier. Alors par définition, il existe un diviseur strict d' de d. Mais alors d' divise n, $d' > 1$ et $d' < d$, ce qui contredit la minimalité de d.

Comme d divise n, on peut écrire $n = dd'$. On a $d > 1$ et comme n n'est pas premier, $d < n$. Ainsi d' est un diviseur de n strictement supérieur à 1. Par minimalité de d, on obtient $d' \geqslant d$ et donc $n \geqslant d^2$ puis finalement $d \leqslant \sqrt{n}$. □

Remarque. On déduit de la propriété précédente que pour tester si un entier $n > 1$ est premier, il suffit de regarder s'il est divisible ou non par un des entiers compris entre 2 et $\sqrt{n}$. Par exemple, pour vérifier que 37 est premier, il suffit de voir qu'il n'est divisible ni par 2, ni par 3, ni par 4, ni par 5, ni par 6. On aurait également pu éviter les divisions par 4 et 6 si on savait par avance que ces nombres étaient composés.

La remarque précédente nous amène à la méthode suivante, appelée *crible d'Ératosthène* pour lister tous les nombres premiers entre 1 et n : on écrit à la suite les uns des autres tous les entiers compris entre 2 et n. On entoure le premier 2 et on barre tous ses multiples (*i.e.* tous les nombres pairs). On entoure ensuite le prochain nombre non barré (en l'occurrence 3) et on barre tous ses multiples. Ainsi de suite jusqu'à $\sqrt{n}$. On entoure finalement les nombres non barrés. Les nombres entourés sont alors exactement les nombres premiers compris entre 1 et n.

Le théorème fondamental de l'arithmétique

On en arrive à présent au théorème fondamental de l'arithmétique. Nous aurons besoin pour la démonstration du lemme suivant (qui sera démontré dans le paragraphe 2.4) :

Lemme 1.2.3 *Si un nombre premier p divise le produit $a_1 \cdots a_n$, alors il divise l'un des a_i.*

Théorème 1.2.4 (Décomposition en facteurs premiers) *Tout entier $n \geqslant 1$ se décompose d'une et d'une seule manière en un produit de nombres premiers. Autrement dit, pour tout entier $n \geqslant 1$, il existe des nombres premiers deux à deux distincts $p_1, \ldots, p_k$ et des entiers strictement positifs $\alpha_1, \ldots, \alpha_k$, uniquement déterminés à l'ordre près, tels que :*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

Remarque. Le théorème reste bien vrai pour $n = 1$: il faut choisir $k = 0$, le produit d'aucun entier étant par convention égal à 1.

Démonstration. Commençons par l'existence de la décomposition. On raisonne par récurrence sur n. Commençons (pour ne pas perturber le lecteur) à $n = 2$ qui s'écrit comme un produit de nombres premiers, étant lui-même premier.

Soit $n \geqslant 3$ un entier. Supposons que tous les entiers strictement inférieurs à n s'écrivent comme le stipule le théorème et montrons que la conclusion subsiste pour l'entier n. Il y a deux cas : soit n est premier, soit il ne l'est pas. Le premier cas est vite réglé : n premier s'écrit bien comme un produit de nombres premiers. Supposons donc que n soit composé. Ainsi, il s'écrit $n = dd'$ avec $2 \leqslant d < n$ et $2 \leqslant d' < n$. Les entiers d et d' relèvent de l'hypothèse de récurrence et on peut écrire :

$$\begin{aligned} d &= p_1 p_2 \cdots p_k \\ d' &= p'_1 p'_2 \cdots p'_{k'} \end{aligned}$$

pour des nombres premiers p_i et p'_i. Il ne reste plus qu'à effectuer le produit pour conclure.

Passons désormais à l'unicité. Supposons que :

$$p_1 p_2 \cdots p_k = p'_1 p'_2 \cdots p'_{k'}$$

pour certains nombres premiers p_i et p'_i. On veut montrer que $k = k'$ et que les p_i sont égaux aux p'_i à l'ordre près. Raisonnons par l'absurde. Parmi les contre-exemples dont on vient de supposer l'existence, il en est au moins un pour lequel $\min(k, k')$ est minimal. Considérons un de ceux-ci.

Le nombre premier p_1 divise le produit $p'_1 p'_2 \cdots p'_{k'}$ donc d'après le lemme 1.2.3, il divise p'_i pour un certain entier i. Or, les diviseurs de p'_i (qui est premier) ne sont que 1 et p'_i. Comme $p_1 \neq 1$, il ne reste plus que la possibilité $p_1 = p'_i = p$. On peut alors simplifier l'égalité :

$$p_1 p_2 \cdots p_k = p'_1 p'_2 \cdots p'_{k'}$$

en divisant par p, obtenant ainsi un contre-exemple plus petit. C'est une contradiction et l'unicité est prouvée. □

Le théorème précédent permet de décrire explicitement les diviseurs d'un entier n dont on connaît la décomposition en facteurs premiers.

Proposition 1.2.5 *Si la décomposition en facteurs premiers de l'entier $n \geqslant 1$ est $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, alors les diviseurs positifs de n sont les entiers de la forme $p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$, avec $0 \leqslant \beta_i \leqslant \alpha_i$ pour tout $1 \leqslant i \leqslant k$.*

Comme conséquence, on obtient une expression du PGCD et du PPCM de deux entiers lorsqu'on connaît leur décomposition en facteurs premiers. Précisément, si :

$$\begin{aligned} a &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \\ b &= p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} \end{aligned}$$

où les p_i sont deux à deux distincts, mais les α_i et β_i sont éventuellement nuls, on a :

$$\begin{aligned} \text{PGCD}\,(a, b) &= p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \cdots p_k^{\min(\alpha_k,\beta_k)} \\ \text{PPCM}\,(a, b) &= p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \cdots p_k^{\max(\alpha_k,\beta_k)} \end{aligned}$$

Si l'on remarque que pour α et β des entiers (ou des réels), on a toujours $\min(\alpha, \beta) + \max(\alpha, \beta) = \alpha + \beta$, on déduit directement des deux expressions précédentes la proposition suivante :

Proposition 1.2.6 *Si a et b sont des entiers positifs, on a l'égalité :*

$$\text{PGCD}\,(a, b) \cdot \text{PPCM}\,(a, b) = ab$$

Infinité des nombres premiers et raffinements

Le premier résultat qui remonte à Euclide est le suivant :

Proposition 1.2.7 *Il existe une infinité de nombres premiers.*

Démonstration. On raisonne par l'absurde. On suppose qu'il n'existe qu'un nombre fini d'entiers premiers, disons $p_1, p_2, \dots, p_k$. On peut alors exhiber un entier qui n'est divisible par aucun de ces nombres premiers, ce qui est contradictoire compte tenu du fait que cet entier possède un diviseur premier. En effet, considérons $N = p_1 p_2 \cdots p_k + 1$: si p_i $(1 \leqslant i \leqslant k)$ divisait n, alors p_i diviserait 1, ce qui est absurde. □

La démonstration précédente s'applique pour obtenir des résultats plus précis comme le montre l'exercice suivant :

<u>*Exercice*</u> : Montrer qu'il existe une infinité de nombres premiers de la forme $4n + 3$.

<u>*Solution*</u> : On raisonne par l'absurde en supposant qu'il n'existe qu'un nombre fini de premiers de cette forme, notés $p_1, p_2, \dots, p_k$. On considère alors $N = 4p_1 p_2 \dots p_k - 1$. Les diviseurs premiers de n sont distincts de 2 et des p_i $(1 \leqslant i \leqslant k)$, et il en existe un qui est de la forme $4n + 3$, car sinon on vérifie immédiatement que N ne pourrait être de la forme $4n + 3$ (un nombre premier qui n'est de la forme $4n + 3$ est de la forme $4n + 1$ et le produit de tels nombres est encore de cette forme). √

Remarque. De même, on peut prouver qu'il existe une infinité de nombres premiers de la forme $6n + 5$. Toutefois, ces cas restent anecdotiques : par exemple, la démonstration

précédente ne s'applique par pour les nombres premiers de la forme $4n+1$ (qui pourtant forment bien un ensemble infini).

Une autre propriété utile qui mesure plus ou moins la raréfaction des nombres premiers est la proposition totalement élémentaire suivante :

Proposition 1.2.8 *Il existe des suites arbitrairement longues de nombres consécutifs composés. Autrement dit, pour tout k, il est possible de trouver un entier n tel que les nombres $n+1, \ldots, n+k$ soient tous composés.*

Démonstration. Il suffit de prendre $n = (k+1)! + 1$. □

Remarque. Comme l'ensemble des nombres premiers est infini, on déduit directement de la proposition précédente, la proposition suivante plus précise :

Proposition 1.2.9 *Pour tout entier k, il existe un nombre premier p tel que tous les nombres $p+1, \ldots, p+k$ soient composés.*

Mis à part ces cas simples, la répartition des nombres premiers est une question qui a occupé les mathématiciens durant des générations, et de nombreuses questions demeurent ouvertes. Citons quelques résultats importants qu'il est bon de connaître même si leur démonstration dépasse de loin le cadre de ce cours :

Propriétés

- ☞ *Postulat de Bertrand.* Pour tout entier $n \geqslant 1$, il existe un nombre premier entre n et $2n$.
- ☞ *Théorème des nombres premiers.* Si on note $\pi(x)$ le nombre d'entiers premiers inférieurs ou égaux à x, on a l'estimation $\pi(x) \sim \frac{x}{\ln x}$ (au sens où le quotient des deux membres tend vers 1 lorsque x tend vers l'infini).
- ☞ *Théorème de Dirichlet.* Si $a \neq 0$ et b sont deux entiers naturels premiers entre eux, la suite $an+b$ (n entier) contient une infinité de nombres premiers.

1.3 Valuation p-adique

Les valuations sont un moyen systématique et souvent efficace pour utiliser toute la puissance du théorème de décomposition en facteurs premiers. Commençons par une définition :

Définition 1.3.1 Si p est un nombre premier, et n un entier non nul, la *valuation p-adique* de n est le plus grand entier k tel que p^k divise n. On la note $v_p(n)$.

Si $n = 0$, on convient que $v_p(0) = +\infty$ pour tout nombre premier p.

Les propriétés suivantes sont élémentaires mais il est bon de toujours les avoir en tête. Leur manipulation est simple et puissante.

Propriétés

- ☞ Si n non nul se décompose sous la forme $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, alors $v_{p_i}(n) = \alpha_i$ pour tout $1 \leqslant i \leqslant k$, et $v_p(n) = 0$ si p est distinct des p_i. Ainsi, $v_p(n) = 0$ sauf pour un nombre fini de p premiers.
- ☞ Si m et n sont deux entiers, m divise n si et seulement si $v_p(m) \leqslant v_p(n)$ pour tout nombre premier p.
- ☞ Si a et b sont des entiers non nuls, on a :

$$\begin{aligned} v_p(\text{PGCD}\,(a,b)) &= \min\,(v_p(a), v_p(b)) \\ v_p(\text{PPCM}\,(a,b)) &= \max\,(v_p(a), v_p(b)) \end{aligned}$$

- ☞ Si m et n sont deux entiers, on a, pour tout nombre premier p :

$$\begin{aligned} v_p(ab) &= v_p(a) + v_p(b) \\ v_p(a+b) &\geqslant \min\,(v_p(a), v_p(b)) \end{aligned}$$

  et la dernière inégalité est une égalité dès que $v_p(a) \neq v_p(b)$.

Il est possible de déterminer les valuations p-adiques d'une factorielle. On rappelle, fort à propos, que par définition $n! = 1 \times 2 \times \cdots \times n$.

Proposition 1.3.2 (Formule de Legendre) *Si p est un nombre premier et n est un entier positif, on a :*

$$v_p(n!) = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right] = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots$$

Remarque. Lorsque $p^i > n$, le nombre $\left[\frac{n}{p^i}\right] = 0$. Ceci assure qu'il n'y a bien qu'un nombre fini de termes non nuls dans la somme précédente.

Démonstration. Pour un entier positif ou nul i, appelons n_i le nombre d'entiers compris entre 1 et n dont la valuation p-adique est *exactement* i. On a alors :

$$v_p(n!) = n_1 + 2n_2 + 3n_3 + \cdots$$

D'autre part, les entiers dont la valuation excède i sont exactement les multiples de p^i et sont au nombre de $\left[\frac{n}{p^i}\right]$, d'où :

$$\left[\frac{n}{p^i}\right] = n_i + n_{i+1} + n_{i+2} + \cdots$$

Les deux formules précédentes mises ensemble démontrent la proposition. □

Classiquement, on illustre le théorème précédent par l'exercice suivant :

<u>*Exercice*</u> : Par combien de zéros se termine le nombre 2004! ?

<u>*Solution*</u> : L'entier 10 n'est pas premier : on ne peut donc pas appliquer directement la formule de Legendre. En décomposant 10 en facteurs premiers, on se rend compte que le

plus grand exposant n tel que 10^n divise 2004! est le plus petit des deux nombres $v_2(2004!)$ et $v_5(2004!)$. La formule de Legendre prouve directement que c'est $v_5(2004!)$. Il vaut :

$$\left[\frac{2004}{5}\right] + \left[\frac{2004}{25}\right] + \left[\frac{2004}{125}\right] + \left[\frac{2004}{625}\right] + \left[\frac{2004}{3125}\right] + \cdots = 400 + 80 + 16 + 3 + 0 + \cdots = 499$$

Le nombre 2004! se termine donc par 499 zéros. $\surd$

1.4 Quelques fonctions arithmétiques

Les principales fonctions arithmétiques sont les suivantes :

☞ la fonction d qui à n associe le nombre de diviseurs positifs de n ;

☞ la fonction σ qui à n associe la somme des diviseurs positifs de n ;

☞ plus généralement, la fonction σ_s qui à n associe les somme des diviseurs positifs de n élevés à la puissance s (les deux cas précédents correspondant à $s = 0$ et $s = 1$) ;

☞ la fonction P qui à n associe le produit des diviseurs positifs de n

Remarque. Les notations introduites précédemment sont traditionnelles mais ne sont pas universelles. Elles seront normalement reprécisées à chaque nouvelle apparition. De même si vous êtes amenés à utiliser ces fonctions, il est souhaitable de redonner rapidement la définition avant pour fixer les notations.

La décomposition en facteurs premiers permet de donner les expressions de ces fonctions arithmétiques :

Proposition 1.4.1 *Si la décomposition en facteurs premiers de n est $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, alors on a les expressions suivantes :*

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$$

$$\sigma_s(n) = \frac{p_1^{s(\alpha_1+1)} - 1}{p_1^s - 1} \cdot \frac{p_2^{s(\alpha_2+1)} - 1}{p_2^s - 1} \cdots \frac{p_k^{s(\alpha_k+1)} - 1}{p_k^s - 1}$$

$$P(n) = n^{\frac{d(n)}{2}}$$

Démonstration. On ne démontre que l'expression de P qui est la plus difficile, les autres se traitant de façon analogue.

Un diviseur positif de n s'écrit $p_1^{\beta_1} \cdots p_k^{\beta_k}$ où $0 \leqslant \beta_i \leqslant \alpha_i$. Le produit de tous ces nombres est de la forme :

$$p_1^{\gamma_1} \cdots p_k^{\gamma_k}$$

Il suffit donc de calculer les exposants γ_i. Fixons un entier $v \in \{0, 1, \dots, \alpha_1\}$. Il y a exactement $(\alpha_2 + 1) \cdots (\alpha_k + 1)$ diviseurs de n pour lesquels $\beta_1 = v$. Lorsque l'on multiplie tous ces diviseurs, on aura donc :

$$\gamma_1 = (\alpha_2 + 1) \cdots (\alpha_k + 1) \sum_{v=0}^{\alpha_1} v = \frac{1}{2}\alpha_1 (\alpha_1 + 1) \cdots (\alpha_k + 1) = \alpha_1 \cdot \frac{d(n)}{2}$$

On a bien entendu une formule analogue pour γ_i. En remettant tout bout à bout, on obtient la formule annoncée. $\square$

Exercice : L'entier $n > 0$ étant fixé, déterminer le nombre de couples (x, y) d'entiers strictement positifs vérifiant $\frac{1}{x} + \frac{1}{y} = \frac{1}{n}$.

Solution : L'équation se réécrit sous la forme :

$$(x - n)(y - n) = n^2$$

Il y a donc autant de solutions que de diviseurs positifs de n^2 en remarquant que puisque $\frac{1}{x} + \frac{1}{y} = \frac{1}{n}$, on a forcément $x > n$ et $y > n$. $\surd$

1.5 Nombres rationnels

Définition 1.5.1 Un *nombre rationnel* est un réel de la forme $\frac{a}{b}$ pour a et b entiers, $b \neq 0$. Leur ensemble se note $\mathbf{Q}$.

Nous allons voir que certaines propriétés des entiers demeurent inchangées sur les rationnels. Précisément il est possible de parler de décomposition en facteurs premiers, et donc de valuation p-adique pour tout nombre premier p.

Théorème 1.5.2 *Soit r un nombre rationnel non nul. Alors r se décompose de façon unique (à permutation des facteurs près) sous la forme :*

$$r = p_1^{\alpha_1} \cdots p_d^{\alpha_d}$$

où les p_i sont des nombres premiers deux à deux distincts et où les α_i sont des entiers relatifs.

Démonstration. La démonstration est une conséquence presque directe de la propriété analogue pour les nombres entiers. Elle est laissée au lecteur. $\square$

Définition 1.5.3 Si p est un nombre premier, on appelle *valuation p-adique* du rationnel $r \neq 0$, et on note $v_p(r)$, l'exposant apparaissant sur le nombre premier p dans la décomposition en facteurs premiers de r. Bien sûr, si p n'apparaît pas dans cette décomposition, on convient que $v_p(r) = 0$.

Si $r = 0$, on convient que $v_p(r) = +\infty$ pour tout nombre premier p.

Propriétés

- ☞ Si r est un rationnel non nul, il n'existe qu'un nombre fini de nombres premiers p pour lesquels $v_p(r) \neq 0$
- ☞ Si $\frac{a}{b}$ est une fraction représentant le rationnel r, alors :

$$v_p(r) = v_p(a) - v_p(b)$$

En particulier, la valeur $v_p(a) - v_p(b)$ ne dépend pas de la fraction choisie.

☞ Soit r un nombre rationnel. Alors r est entier si, et seulement si $v_p(r) \geqslant 0$ pour tout nombre premier p.

☞ Soient s et t deux nombres rationnels, on a :

$$\begin{array}{rcl} v_p(st) & = & v_p(s) + v_p(t) \\ v_p(s+t) & \geqslant & \min(v_p(s), v_p(t)) \end{array}$$

et la dernière inégalité est une égalité dès que $v_p(s) \neq v_p(t)$.

Les extensions précédentes permettent par exemple de démontrer simplement l'irrationalité de $\sqrt{2}$. En effet, si $\sqrt{2}$ était rationnel, on devrait avoir, du fait de l'égalité $\left(\sqrt{2}\right)^2 = 2$:

$$2 \cdot v_2\left(\sqrt{2}\right) = 1$$

soit $v_2\left(\sqrt{2}\right) = \frac{1}{2}$, mais cela n'est pas possible puisque les valuations p-adiques sont toujours entières.

En utilisant les mêmes concepts, on peut résoudre l'exercice suivant :

Exercice : Montrer que si $n \geqslant 2$ et $a > 0$ sont des entiers, alors $\sqrt[n]{a}$ est soit un entier, soit un nombre irrationnel.

Solution : Supposons que $\sqrt[n]{a}$ soit un nombre rationnel. On peut alors écrire pour tout nombre premier p :

$$nv_p\left(\sqrt[n]{a}\right) = v_p(a)$$

et donc $v_p\left(\sqrt[n]{a}\right) = \frac{1}{n} v_p(a) \geqslant 0$ puisque a est entier. Cela démontre que $\sqrt[n]{a}$ est un entier. $\checkmark$

Densité

Une propriété des rationnels souvent utiles pour les passages à la limite (et donc finalement assez peu en arithmétique) est donnée par le théorème suivant :

Théorème 1.5.4 *Soit $\varepsilon > 0$ et $x \in \mathbf{R}$. Alors il existe $y \in \mathbf{Q}$ tel que $|x - y| \leqslant \varepsilon$.*
On dit, dans cette situation, que $\mathbf{Q}$ est dense *dans $\mathbf{R}$.*

Démonstration. Soit q un entier strictement supérieur à $\frac{1}{\varepsilon}$ et $p = [qx]$. On a l'encadrement $p \leqslant qx \leqslant p + 1$ et donc en divisant par q :

$$\frac{p}{q} \leqslant x \leqslant \frac{p}{q} + \frac{1}{q} < \frac{p}{q} + \varepsilon$$

Ainsi le rationnel $y = \frac{p}{q}$ convient. $\square$

1.6 Exercices

Exercice 1 On désigne par $d(n)$ le nombre de diviseurs strictement positifs de l'entier n. Montrer que $d(n)$ est impair si, et seulement si n est un carré.

Exercice 2 (Saint-Petesbourg 04) Déterminer tous les entiers positifs n tels que $5^{n-1} + 3^{n-1}$ divise $5^n + 3^n$.

Exercice 3 Montrer que pour tout entier n, le nombre $n^3 - n$ est un multiple de 6.

Exercice 4 (OIM 59) Montrer que la fraction $\frac{21n+4}{14n+3}$ est toujours irréductible.

Exercice 5 Montrer que $2x + 3$ est un multiple de 11 si, et seulement si $5x + 2$ l'est.

Exercice 6 Soit $p > 3$ un nombre premier. Montrer que $p^2 - 1$ est un multiple de 12.

Exercice 7 Soient a et b des entiers strictement positifs tels que a^n divise b^{n+1} pour tout entier $n \geqslant 1$. Montrer que a divise b.

Exercice 8 Soit n un entier strictement positif. On appelle k le nombre de diviseurs premiers de n. Prouver que :

$$\log n \geqslant k \log 2$$

Exercice 9 Soient p un nombre premier et n un entier tels que p divise n^k. Est-ce qu'alors, forcément, p divise n ?

Exercice 10* (Baltique 04) Déterminer tous les ensembles X d'entiers strictement positifs contenant au moins deux éléments et tels que, si m et n sont dans X avec $n > m$ alors il existe un élément $k \in X$ vérifant $n = mk^2$.

Exercice 11* (Irlande 98) Déterminer les entiers n ayant exactement 16 diviseurs :

$$1 = d_1 < d_2 < \ldots < d_{15} < d_{16} = n$$

et tels que $d_6 = 18$ et $d_9 - d_8 = 17$.

Exercice 12* Déterminer tous les entiers a, b et c strictement supérieurs à 1 tels que a divise $bc - 1$, b divise $ca - 1$ et c divise $ab - 1$.

Exercice 13* Pierre et Xavier jouent au jeu suivant. Ils commencent par choisir un nombre entier $n > 0$. Puis, Pierre choisit en secret un entier m tel que $0 < m < n$. Xavier doit alors découvrir le nombre secret. Pour cela, il peut proposer un nombre k quelconque à Pierre qui, en retour, lui indique si le nombre $m + k$ est premier ou non. Prouver que Xavier peut déterminer le nombre secret de Pierre en moins de $n - 1$ questions.

Exercice 14* Montrer que les racines cubiques de trois nombres premiers distincts ne peuvent être dans une même progression arithmétique.

Exercice 15* Soit x un réel. Est-il vrai que :

a) Si x^7 et x^{12} sont rationnels alors x est rationnel ?
b) Si x^9 et x^{12} sont rationnels alors x est rationnel ?

Exercice 16* (d'après Autriche 02) Soit $a \geqslant 9$ un entier impair. Montrer que l'équation :

$$x^{[x]} = \frac{a}{2}$$

n'a pas de solution pour $x \in \mathbf{Q}$.

Exercice 17* Trouver le plus petit entier x tel que $2|x-1, 3|x-2, \ldots, 9|x-8$.

Exercice 18* (OIM 02) Les diviseurs strictement positifs de l'entier $n > 1$ sont $1 = d_1 < d_2 < \ldots < d_k = n$. Soit $d = d_1 d_2 + d_2 d_3 + \ldots + d_{k-1} d_k$. Montrer que $d < n^2$ et trouver tous les n pour lesquels d divise n^2.

Exercice 19* (Nombres de Fermat) Montrer que si $2^n + 1$ est un nombre premier, alors n est une puissance de 2.

Exercice 20* Si $n > 1$ est un entier, on note $d(n)$ le nombre de ses diviseurs positifs, $\sigma(n)$ la somme de ses diviseurs positifs ou $\varphi(n)$ le nombre de nombres premiers avec n et compris entre 1 et n.

Trouver tous les entiers $n > 1$ tels que :

$$\sigma(n) + \varphi(n) = n \cdot d(n)$$

Exercice 21* (OIM 68) Le symbôle $[x]$ désignant la partie entière de x. Calculer :

$$\left[\frac{n+1}{2}\right] + \left[\frac{n+2}{4}\right] + \left[\frac{n+4}{8}\right] + \ldots + \left[\frac{n+2^k}{2^{k+1}}\right] + \ldots$$

Exercice 22* On note p_n le n-ième nombre premier. En utilisant le théorème des nombres premiers, montrer que $p_n \sim n \log n$.

Exercice 23* (APMO 04) Déterminer toutes les parties E non vides de $\mathbf{N}^\star$ telles que pour tous a et b dans E, le nombre $\frac{a+b}{\text{PGCD}(a,b)}$ est aussi dans E.

Exercice 24* Trouver tous les entiers n strictement positifs pour lesquels 2^n divise $3^n - 1$.

Exercice 25* (USA 72) Soient a, b et c des entiers strictement positifs. Montrer que :

$$\frac{\text{PGCD}(a,b,c)^2}{\text{PGCD}(a,b)\,\text{PGCD}(b,c)\,\text{PGCD}(a,c)} = \frac{\text{PPCM}(a,b,c)^2}{\text{PPCM}(a,b)\,\text{PPCM}(b,c)\,\text{PPCM}(a,c)}$$

Exercice 26* (Iran 96) Soit $k > 0$ un entier. Prouver que tout entier $n > 0$ peut s'écrire de façon unique sous la forme :

$$n = \mathrm{C}_{a_k}^{k} + \mathrm{C}_{a_{k-1}}^{k-1} + \cdots + \mathrm{C}_{a_t}^{t}$$

où $a_k > a_{k-1} > \cdots > a_t \geqslant t \geqslant 1$ sont des entiers.

Exercice 27* (Erdös) Soient $a_1, \ldots, a_{n+1}$ des entiers deux à deux distincts dans $\{1, \ldots, 2n\}$.

a) Montrer qu'il existe i et j tels que a_i est premier avec a_j.

b) Montrer qu'il existe i et j distincts tels que a_i divise a_j.

Exercice 28* (Australie 96) Si n est un entier, on note $\sigma(n)$ la somme des diviseurs positifs de n. Soit (n_i) une suite strictement croissante d'entiers telle que $\sigma(n_i) - n_i$ est constante. Montrer que tous les n_i sont premiers.

Exercice 29* (Iran 99) Déterminer les entiers n pour lesquels $d_1^2 + d_2^2 + d_3^2 + d_4^2 = n$ où $1 = d_1 < d_2 < d_3 < d_4$ désignent les quatre plus petits diviseurs de n.

Exercice 30* Soient (a_n) et (b_n) deux suites d'entiers. On suppose que les suites $(a_n + b_n)$ et $(a_n b_n)$ sont arithmétiques. Montrer qu'il existe une constante c tel que pour tout n, on ait $a_n = c$ ou $b_n = c$.

Exercice 31* (Corée 98) Trouver tous les entiers strictement positifs ℓ, m, n premiers entre eux deux à deux tels que :

$$(\ell + m + n)\left(\frac{1}{\ell} + \frac{1}{m} + \frac{1}{n}\right)$$

soit un entier.

Exercice 32* (Fonction de Moëbius) On définit la *fonction de Moëbius* par $\mu(1) = 1$, $\mu(n) = 0$ est n est divisible par p^2 pour un certain nombre premier p, et $\mu(p_1 \cdots p_r) = (-1)^r$ si les p_i sont des nombres premiers deux à deux distincts.

a) Montrer que pour tout $n > 1$, on a :

$$\sum_{d|n} \mu(d) = 0$$

b) En déduire que si $f : \mathbf{N}^\star \to \mathbf{N}^\star$ est une fonction et si g est définie par la formule :

$$g(n) = \sum_{d|n} f(d)$$

alors on peut retrouver f à partir de g grâce à la formule :

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$$

Exercice 33* Prouver que parmi dix entiers consécutifs, il y en a un qui est premier avec chacun des autres.

Exercice 34* (AMM) Si n est un entier, on note $P(n)$ le produit des diviseurs de n. Montrer que si $P(n) = P(m)$ alors $n = m$.

Exercice 35* Déterminer tous les entiers n et m strictement positifs pour lesquels la somme des entiers de n jusqu'à $n+m$ vaut 1000.

Exercice 36* Déterminer toutes les suites $(a_n)\,(n \geqslant 1)$ d'entiers strictement positifs telle que $\text{PGCD}\,(a_i, a_j) = \text{PGCD}\,(i, j)$ pour tous indices i et j.

Exercice 37* (Nombres de Mersenne) Montrer que si $2^n - 1$ est un nombre premier, alors n est également premier.

Exercice 38* (URSS 61) Prouver que parmi 39 entiers consécutifs, on peut toujours en trouver un dont la somme des chiffres (écriture décimale) est divisible par 11.

Est-ce encore vrai pour 38 entiers consécutifs ?

Exercice 39 (Putnam 83)** Déterminer un nombre réel $x > 0$ tel que, pour tout entier $n > 0$, le nombre $[x^n]$ a la même parité que n.

Exercice 40 (SL 96)** Construire une fonction $f : \mathbf{N} \to \mathbf{N}$ bijective et vérifiant :

$$f\,(3mn + m + n) = 4f\,(m)\,f\,(n) + f\,(m) + f\,(n)$$

pour tous entiers m et n.

Exercice 41** En utilisant le théorème de répartition des nombres premiers, montrer que l'ensemble :

$$\left\{\frac{p}{q},\ p \text{ et } q \text{ premiers}\right\}$$

est dense dans $\mathbf{R}^+$.

Exercice 42 (Moscou 95)** Montrer qu'il existe une infinité d'entiers composés n pour lesquels n divise $3^{n-1} - 2^{n-1}$.

Exercice 43 (Théorème de Miller)** Montrer qu'il existe un réel x tel que la suite définie par $x_0 = x$ et $x_{n+1} = 2^{x_n}$ est telle que pour tout n, $[x_n]$ est un nombre premier. (On pourra utiliser le postulat de Bertrand).

Exercice 44 (OIM 75)** Peut-on placer 1975 points sur le cercle unité dont les distances deux à deux sont toutes rationnelles ?

Exercice 45** On note $\sigma\,(n)$ la somme des diviseurs positifs de l'entier n. Pour tout entier $p > 0$, on pose :

$$f\,(m) = \max\left\{n \in \mathbf{N}^\star \,/\, \sigma\,(n) \leqslant m\right\}$$

Montrer que, pour tout entier $k > 0$, l'équation $m - f(m) = k$ a une infinité de solutions.

Exercice 46 (Chine 88)** Déterminer le plus petit $n > 3$ pour lequel pour toute écriture $\{3, \ldots, n\} = A \cup B$, l'équation $xy = z$ a une solution pour x, y et z non nécessairement distincts, et tous les trois dans A ou tous les trois dans B.

Exercice 47** Soit $p \geqslant 5$ un nombre premier. Calculer :

$$\sum_{k=1}^{p-1} \left[\frac{k^3}{p}\right] \qquad \text{et} \qquad \sum_{k=1}^{(p-1)(p-2)} \left[\sqrt[3]{kp}\right]$$

Exercice 48 (Italie 04) a)** Montrer qu'il existe 2004 puissances parfaites distinctes en progression arithmétique.

b) Est-il possible de trouver une suite arithmétique infinie formée exclusivement de puissances parfaites ?

Exercice 49** Soit $n > 0$ un entier. Montrer qu'il n'existe pas de rationnels x et y tels que :

$$x + y + \frac{1}{x} + \frac{1}{y} = 3n$$

Exercice 50 (Moldavie 96)** Soit $n = 2^{13} \times 3^{11} \times 5^7$. Déterminer le nombre de diviseurs de n^2 inférieurs à n et ne divisant pas n.

Exercice 51** Soient a, b et c des entiers strictement positifs, premiers entre eux dans leur ensemble, et tels que :

$$\frac{1}{a} + \frac{1}{b} = \frac{1}{c}$$

Prouver que $a + b$ est un carré parfait.

Exercice 52** Un nombre n est dit *parfait* si $\sigma(n) = 2n$ (où σ désigne la somme des diviseurs positifs). Montrer que :

a) (Euler) l'entier n est parfait pair si et seulement s'il est de la forme $2^{k-1}\left(2^k - 1\right)$ avec $2^k - 1$ premier ;

b) (Sylvester) si n est parfait impair, alors il possède au moins trois diviseurs premiers distincts.

Exercice 53 (TDV 99)** Montrer que si a et b sont des entiers tels que $\text{PPCM}(a, a+5) = \text{PPCM}(b, b+5)$ alors $a = b$.

Existe-t-il des entiers strictement positifs a, b et c tels que $\text{PPCM}(a, b) = \text{PPCM}(a+c, b+c)$?

Exercice 54** Soient a, b et c des entiers strictement positifs tels que :

$$\frac{a}{b} + \frac{b}{c} + \frac{c}{a}$$

est entier. Montrer que abc est un cube.

Exercice 55** Soit n un entier. On suppose que $n = ab = cd$ pour certains entiers positifs a, b, c et d. Montrer que $a^k + b^k + c^k + d^k$ est un entier composé pour tout entier k positif.

Exercice 56 (OIM 94)** Trouver tous les couples (m, n) d'entiers strictement positifs tel que :

$$\frac{n^3 + 1}{mn - 1}$$

soit entier.

Exercice 57 (SL 99)** Montrer que tout rationnel strictement positif peut s'écrire sous la forme :

$$\frac{a^3 + b^3}{c^3 + d^3}$$

pour certains entiers a, b, c et d strictement positifs.

Exercice 58** Montrer que tout rationnel compris strictement entre 0 et 1 peut s'écrire sous la forme :

$$\frac{1}{n_1} + \ldots + \frac{1}{n_k}$$

pour certains entiers n_i deux à deux distincts.

Exercice 59 (Balkans 96)** Soit $p > 5$ un nombre premier. On définit :

$$S = \left\{p - n^2,\, n \in \mathbf{N}, n^2 < p\right\}$$

Prouver qu'il existe a et b dans S tels que $1 < a < b$ et a divise b.

Exercice 60 (OIM 87)** On considère le plan euclidien. Soit $n \geqslant 3$ un entier. Montrer qu'il existe n points vérifiant :
(1) trois quelconques de ces points ne sont pas alignés
(2) la distance entre deux quelconques de ces points est irrationnelle
(3) l'aire du triangle déterminé par trois quelconques de ces points est rationnelle.

Exercice 61 (APMO 98)** Trouver le plus grand entier n qui soit divisible par tous les entiers inférieurs ou égaux à $\sqrt[3]{n}$.

Exercice 62 (OIM 92)** Trouver tous les entiers a, b, c vérifiant $1 < a < b < c$ et tels que $(a-1)(b-1)(c-1)$ divise $abc - 1$.

Exercice 63 (Inde 98)** Soit M un entier strictement positif. On note :

$$S = \left\{n \in \mathbf{N},\, M^2 \leqslant n < (M+1)^2\right\}$$

Montrer que les produits ab pour a et b dans S sont deux à deux distincts.

Exercice 64** Pour tout entier $n > 0$, on pose :

$$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$$

Montrer que H_n est entier si, et seulement si $n = 1$. Déterminer les entiers m et n pour lesquels la différence $H_{m+n} - H_m$ est entière ?

Exercice 65** Soient $a < b \leqslant c < d$ des entiers tels que $ad = bc$ et $\sqrt{d} - \sqrt{a} \leqslant 1$. Prouver que a est un carré.

Exercice 66 (OIM 83)** Soient a, b et c des entiers strictement positifs et premiers entre eux deux à deux. Montrer que $2abc - ab - bc - ca$ est le plus grand entier qui ne peut pas s'écrire sous la forme $xbc + yca + zab$ avec x, y, z entiers positifs ou nuls.

Exercice 67 (Putnam 95)** Pour α un réel strictement positif, on note $S(\alpha) = \{[n\alpha], n \in \mathbf{N}^\star\}$. Montrer que $\mathbf{N}^\star$ ne peut pas s'écrire comme union disjointe de $S(\alpha)$, $S(\beta)$ et $S(\gamma)$ pour trois réels strictement positifs α, β et γ.

Exercice 68** Montrer qu'il n'existe pas de partie $X \subset \mathbf{N}$ infinie telle que pour toute partie finie $I \subset X$, le nombre $\sum_{x \in I} x$ soit un carré parfait.

Exercice 69 (CG 92)** Quelle est le chiffre des unités du nombre suivant :

$$\left[\frac{10^{1992}}{10^{83}+7}\right]$$

Exercice 70* (Yakusk 00)** Prouver qu'il n'existe pas d'entiers $n > 0$ et $a_1 < \ldots < a_k$ tels que :

$$\frac{1}{a_1!} + \cdots + \frac{1}{a_k!} = \frac{1}{10^n}$$

Exercice 71* (OIM 98)** Pour tout entier n strictement positif, $d(n)$ désigne le nombre de diviseurs positifs de n (y compris 1 et n). Trouver tous les entiers strictement positifs k pour lesquels il existe n tel que :

$$\frac{d(n^2)}{d(n)} = k$$

Exercice 72* (OIM 84)** Soient a, b, c et d des entiers positifs impairs vérifiant $a < b < c < d$, $ad = bc$ et $a + d = 2^k$, $b + c = 2^m$ pour deux entiers k et m. Prouver que $a = 1$.

2 Division euclidienne et conséquences

2.1 Division euclidienne et décomposition en base b

Les principales propriétés arithmétiques des entiers découlent de l'existence de la *division euclidienne.*

Théorème 2.1.1 (Division euclidienne) *Soit b un entier non nul. Tout entier a s'écrit de manière unique sous la forme $a = bq + r$, avec q entier et $0 \leqslant r < |b|$. Les entiers q et r sont appelés respectivement* quotient *et* reste *de la division euclidienne de a par b.*

Remarque. Ainsi a est divisible par b si et seulement si $r = 0$.

Comme pour les parties entières, on prendra garde à ce qui se produit lorsque l'un des nombres a et b est négatif.

Démonstration. Montrons tout d'abord l'existence. On peut supposer $b > 0$ dans un premier temps. On prend alors $q = \left[\frac{a}{b}\right]$ et $r = a - bq$. De l'inégalité $q \leqslant \frac{a}{b} < q+1$, on déduit aisément $0 \leqslant r < b$. Si $b < 0$, on se ramène au cas précédent en considérant $-b$.

En ce qui concerne l'unicité, si a s'écrit $a = bq + r = bq' + r'$, alors $b(q - q') = r' - r$ donc b divise $r' - r$. Comme $|b| > |r' - r|$, nécessairement $r' - r = 0$, d'où $r' = r$ puis $q' = q$. $\square$

Théorème 2.1.2 (Décomposition en base b) *Soit $b \geqslant 2$ un entier. Tout entier $a \geqslant 0$ s'écrit de façon unique sous la forme :*

$$a = a_0 + a_1 b + a_2 b^2 + \cdots + a_k b^k$$

où k est un entier, les a_i sont des entiers compris entre 0 et $b - 1$ et où $a_k \neq 0$.

On note parfois $a = \overline{a_k a_{k-1} \ldots a_0}^b$. Cette notation est l'écriture en base b *de a.*

Remarque. Dans le cas où $b = 10$, les a_i correspondent exactement aux chiffres usuels de a. On s'aperçoit que 10 ne joue pas un rôle particulier vis-à-vis de la représentation des nombres : par exemple, on aurait pu noter 143 au lieu de 80 si on avait décidé de compter en base 7.

Démonstration. La méthode consiste à effectuer des divisions euclidiennes (par b) successives. On commence par écrire $a = bq_0 + a_0$ avec $a_0 \in \{0, 1, \ldots, b-1\}$. Si $q_0 = 0$, on a fini ! Sinon, on continue nos divisions en écrivant $q_0 = bq_1 + a_1$ avec $a_1 \in \{0, 1, \ldots, b-1\}$. On a alors :

$$a = a_0 + a_1 b + q_1 b^2$$

De même si $q_1 = 0$, on a fini. Sinon on continue, construisant ainsi a_3, a_4 et ainsi de suite. On obtient successivement des égalités du type :

$$a = a_0 + a_1 b + \cdots + a_i b^i + q_i b^{i+1}$$

La suite des q_i est une suite d'entiers positifs strictement décroissante. Elle doit donc s'arrêter, ce qu'ici ne peut être réalisé que si $q_i = 0$. À ce moment, on a bien la décomposition annoncée.

Reste à prouver l'unicité. Supposons que l'on puisse écrire :

$$a_0 + a_1 b + \cdots + a_k b^k = a'_0 + a'_1 b + \cdots + a'_k b^k$$

pour des entiers a_i et a'_i compris entre 0 et $b-1$. Alors $a_0 - a'_0$ est un multiple de b et $|a_0 - a'_0| < b$. D'où $a_0 = a'_0$. On simplifie alors par a_0, puis on divise par b. En appliquant le même argument que précédemment, on obtient $a_1 = a'_1$ et ainsi de suite. $\square$

Ci-dessous, on présente un moyen pratique d'effectuer les calculs pour calculer la décomposition d'un nombre en base b. Ici $a = 80$ et $b = 7$:

$$\begin{array}{r|l}
80 & 7 \\ \cline{2-2}
\mathbf{3} & 11 \,|\, 7 \\ \cline{2-2}
 & \mathbf{4} \,|\, \mathbf{1}
\end{array}$$

En lisant les restes à l'envers, on obtient l'écriture de 80 en base 7, en l'occurrence $80 = \overline{143}^7$.

L'écriture en base b permet de reformuler le théorème de Legendre qui donne la valuation p-adique d'une factorielle :

Théorème 2.1.3 *Soit p un nombre premier. Soit n un entier naturel. On a :*

$$v_p(n!) = \frac{n - s_p(n)}{p-1}$$

où $s_p(n)$ désigne la somme des chiffres de n en base p.

Démonstration. Considérons la décomposition de n en base p :

$$n = n_d p^d + n_{d-1} p^{d-1} + \cdots + n_1 p + n_0$$

Alors, pour tout entier i, on a :

$$\left[\frac{n}{p^i}\right] = n_i + n_{i+1} p + \cdots + n_d p^{d-i}$$

Donc, d'après la formule de Legendre, on a :

$$\begin{aligned}
v_p(n!) &= \left(n_1 + n_2 p + \cdots + n_d p^{d-1}\right) \\
&\qquad + \left(n_2 + n_3 p + \cdots + n_d p^{d-2}\right) + \cdots + (n_{d-1} + n_d p) + (n_d) \\
&= n_1 + n_2 (1+p) + \cdots + n_d \left(1 + p + \cdots + p^{d-1}\right) \\
&= \frac{n_1 (p-1) + n_2 (p^2 - 1) + n_d \left(p^d - 1\right)}{p-1} \\
&= \frac{n - s_p(n)}{p-1}
\end{aligned}$$

$\square$

L'énoncé du théorème sous-entend que $p-1$ divise toujours la quantité $n - s_p(n)$, ce qui peut se voir facilement par ailleurs. En effet, la factorisation :

$$p^k - 1 = (p-1)\left(p^{k-1} + \cdots + p + 1\right)$$

prouve que $p-1$ divise toujours $p^i - 1$. Par ailleurs, on a, en gardant les notations du théorème :

$$n - s_p(n) = n_d\left(p^d - 1\right) + n_{d-1}\left(p^{d-1} - 1\right) + \cdots + n_1(p-1)$$

et la conclusion en découle directement. On remarque en particulier que la primalité de p n'intervient pas pour cette dernière propriété. Bref, on vient de prouver la proposition suivante parfois utile :

Proposition 2.1.4 *Soit $b \geqslant 2$ un entier. Si $s_b(n)$ désigne la somme des chiffres de l'entier n écrit en base b, alors le nombre $s_b(n) - n$ est toujours un multiple de $b-1$.*

Décomposition en base b des nombres rationnels

Soit $b \geqslant 2$ un entier. Si x est un nombre réel, on peut définir sa décomposition en base b : un moyen économique est de définir le n-ième chiffre après la virgule de x comme le dernier chiffre de l'entier $[b^n x]$ ou autrement dit le reste de la division euclidienne de $[b^n x]$ par b.

Théorème 2.1.5 *L'entier b est toujours fixé. Un nombre réel x est rationnel si, et seulement si sa décomposition en base b est périodique à partir d'un certain rang.*

Démonstration. Nous n'allons pas démontrer ce théorème, mais plutôt mettre en valeur les idées sous-jacentes de la preuve.

Supposons pour simplifier que $b = 10$ (cela ne change en rien les choses). Nous partons d'un rationnel $r = \frac{x}{y}$ et nous voulons prouver que sa décomposition en base 10 est périodique à partir d'un certain rang. Pour cela, il suffit de poser la division de x par y. Supposons pour exemple que $x = 5$ et $y = 14$. On écrit :

5	14
50	0 , 357 142 85
80	
100	
20	
60	
40	
120	
80	
10	

On retombe finalement sur un reste déjà rencontré (ce qui est automatique étant donné qu'il n'y a qu'un nombre fini (en l'occurrence y) de restes possibles), et donc on retrouve les mêmes décimales lorsque l'on poursuit l'opération. L'écriture décimale est périodique.

Réciproquement supposons que l'on dispose d'un réel x donc l'écriture décimale est périodique à partir d'un certain rang. Prenons à nouveau un exemple. Au hasard $x =$

$0\,,\,410\;784\;153\;153\;\overline{153}$ (la partie surlignée étant celle qui se répètera). On cherche une fraction qui soit égale à x. Pour cela, on écrit :

$$\begin{array}{rrcl} & 1000x & = & 410\,,\,784\,153\,153\,\overline{153} \\ - & x & = & 0\,,\,410\,784\,153\,\overline{153} \\ \hline & 999x & = & 410\,,\,373\,216 \end{array}$$

ce qui fournit $x = \frac{410\,,\,373\,216}{999} = \frac{410\,373\,216}{999\,000\,000} = \frac{34\,197\,773}{83\,250\,000}$ et qui permet de conclure. Le cas général fonctionne exactement de la même manière. □

Remarque. Comme nous l'avons vu dans l'exemple précédent, l'écriture en base b des chiffres après la virgule d'un nombre rationnel est périodique *à partir d'un certain rang* et pas forcément dès le premier chiffre. En réalité, on peut démontrer que la suite des chiffres après la virgule en base b d'un nombre rationnel r est périodique dès le premier chiffre si, et seulement si r peut se mettre sous la forme $r = \frac{x}{y}$ avec y premier avec b.

2.2 Algorithme d'Euclide

L'algorithme d'Euclide est une méthode efficace pour déterminer le PGCD de deux entiers donnés. Il est basé sur l'égalité suivante :

$$\text{PGCD}\,(a, b) = \text{PGCD}\,(b, r)$$

si $a = bq+r$ pour des entiers a, b, q et r. La démonstration de cette propriété est immédiate.

L'algorithme fonctionne alors ainsi. Supposons donnés deux entiers a et b positifs tels que $a \geqslant b$. On effectue la division euclidienne de a par b :

$$a = bq_0 + r_0$$

et d'après la propriété précédente, on est ramené à calculer le PGCD des entiers b et r_0. Deux cas se présentent alors : si $r_0 = 0$, le PGCD cherché est b. Sinon, on effectue la division euclidienne de b par r_0 :

$$b = r_0 q_1 + r_1$$

et le PGCD cherché vaut celui de r_0 et r_1. Si $r_1 = 0$, on a fini. Sinon, on continue...

Les r_i forment une suite d'entiers positifs ou nuls strictement décroissante (d'après les propriétés de la division euclidienne). Cette suite ne peut pas être infinie, ce qui prouve que l'algorithme doit s'arrêter. La description de cet algorithme prouve qu'il s'arrête automatiquement avec un reste nul. À ce moment, le précédent reste fournit le PGCD cherché.

Examinons un exemple. Supposons que l'on désire calculer le PGCD des entiers 56 et 98. On constitue la liste suivante :

$$98\,,\,56\,,\,42\,,\,14\,,\,0$$

où les deux premiers nombres sont ceux dont on veut calculer le PGCD et où les autres sont obtenus en calculant le reste de la division euclidienne des deux nombres qui les précèdent immédiatement. Le PGCD est le dernier entier non nul ainsi écrit ; ici, c'est 14.

L'algorithme précédent est également tout à fait adapté pour le calcul de $\text{PGCD}\,(a^n - 1, a^m - 1)$ lorsque $a \geqslant 2$, $m \geqslant 1$ et $n \geqslant 1$ sont des entiers. En effet, si la division euclidienne de n par m s'écrit :

$$n = mq + r$$

alors la division euclidienne de $a^n - 1$ par $a^m - 1$ s'écrit :

$$a^n - 1 = (a^m - 1)\left(a^{(q-1)m+r} + a^{(q-2)m+r} + \cdots + a^r\right) + (a^r - 1)$$

et donc en itérant, on obtient la proposition suivante :

Proposition 2.2.1 *Soient a, m et n des entiers strictement positifs. Alors on a l'égalité :*

$$\text{PGCD}\,(a^n - 1, a^m - 1) = a^{\text{PGCD}(m,n)} - 1$$

En particulier, on constate que l'algorithme d'Euclide peut être utilisé pour déterminer des PGCD même si les nombres auxquels on s'intéresse ne sont pas donnés sous forme de valeurs numériques.

2.3 Algorithme d'Euclide étendu et théorème de Bézout

À chaque étape de l'algorithme d'Euclide, on a une égalité de la forme :

$$r_{i-2} = r_{i-1}q_i + r_i$$

où par convention $r_{-2} = a$ et $r_{-1} = b$. À l'avant-dernière étape, on a $r_k = d = \text{PGCD}\,(a, b)$ et donc une égalité de la forme :

$$r_{k-2} = r_{k-1}q_k + d$$

soit encore :

$$d = r_{k-2} - r_{k-1}q_k$$

À l'étape précédente, on a de même :

$$r_{k-1} = r_{k-3} - r_{k-2}q_{k-1}$$

et donc en réinjectant, on obtient une expression de d comme une combinaison linéaire de r_{k-3} et r_{k-2}. En continuant à remonter, on trouve finalement une égalité de la forme :

$$d = ur_{-2} + vr_{-1} = au + bv$$

pour des entiers u et v. On en déduit le théorème suivant que nous avons déjà mentionné (voir paragraphe 1.1) :

Théorème 2.3.1 (Bézout) *Soient a et b des entiers non simultanément nuls. Notons $d = \text{PGCD}\,(a, b)$. Alors il existe des entiers u et v tels que :*

$$d = au + bv$$

En particulier, a et b sont premiers entre eux si, et seulement s'il existe des entiers u et v tels que $au + bv = 1$.

Il existe une présentation des calculs pour déterminer efficacement et sans s'embrouiller les coefficients u et v mentionnés précédemment. On dessine un tableau de quatre colonnes que l'on commence à remplir comme suit :

Quotient	**Reste**	**a**	**b**
	a	1	0
	b	0	1

Les lignes suivantes sont obtenues comme l'explique le schéma suivant :

Quotient	**Reste**	**a**	**b**
$\vdots$	$\vdots$	$\vdots$	$\vdots$
	r_{n-2}	u_{n-2}	v_{n-2}
	r_{n-1}	u_{n-1}	v_{n-1}
q_n	r_n	$u_{n-2} - q_n u_{n-1}$	$v_{n-2} - q_n v_{n-1}$

où q_n et r_n désignement respectivement le quotient et le reste de la division euclidienne de r_{n-2} par r_{n-1}. On remarque déjà dans un premier temps que la colonne des restes correspond exactement aux résultats successifs du calcul explicité dans le paragraphe précédent. Ainsi le dernier reste non nul fournit le PGCD de a et b. Par ailleurs, on vérifie par récurrence qu'à chaque ligne, on a :

$$r_n = u_n a + v_n b$$

ce qui nous donne une expression du PGCD comme combinaison linéaire de a et de b.

Regardons l'exemple $a = 153$ et $b = 71$. En suivant les consignes précédentes, on dessine le tableau suivant :

Quotient	**Reste**	**a**	**b**
	153	1	0
	71	0	1
2	11	1	-2
6	5	-6	13
2	1	13	-28
5	0		

obtenant finalement :

$$1 = 13 \times 153 - 28 \times 71$$

2.4 Lemme de Gauss et conséquences

Le théorème de Bézout implique un autre résultat important :

Théorème 2.4.1 (Lemme de Gauss) *Si des entiers a, b et c sont tels que a divise bc et a est premier avec b, alors a divise c.*

Démonstration. Comme a est premier avec b, on peut écrire $au + bv = 1$ pour des entiers u et v. Ainsi $auc + bvc = c$ et comme a divise auc (car il divise a) et bvc (car il divise bc), il divise la somme qui vaut c. □

Une première conséquence du lemme de Gauss est le lemme 1.2.3 utilisé lors de la preuve de l'unicité de la décomposition en facteurs premiers, à savoir :

Lemme 2.4.2 *Si un nombre premier p divise le produit $a_1 \cdots a_n$, alors il divise l'un des a_i.*

Démonstration. Supposons que p ne divise aucun des a_i. Comme les seuls diviseurs positifs de p sont 1 et p, les nombres p et a_1 sont forcément premiers entre eux. On en déduit, par le lemme de Gauss, que p divise $a_2 \cdots a_n$ (puisque p est premier avec a_1). Ensuite, p divise $a_3 \cdots a_n$, puis en itérant il divise a_n, ce qui est supposé faux. □

Deux autres conséquences très importantes et très utiles du lemme de Gauss sont données respectivement en proposition et en exercice :

Proposition 2.4.3 *Si deux entiers premiers entre eux a et b divisent n, alors le produit ab divise également n.*

Démonstration. Comme a divise n, on peut écrire $n = ak$ pour un certain entier k. Mais alors b divise ak et comme il est premier avec a, il divise k. Ainsi $k = bk'$ pour un entier k' et puis $n = abk'$, ce qui prouve bien que ab divise n. □

Exercice : Soient a et b deux entiers premiers entre eux. On note x_0 et y_0 des entiers tels que $ax_0 + by_0 = 1$. Soit d un entier. Trouver tous les entiers x et y vérifiant :

$$ax + by = d$$

Solution : On remarque dans un premier temps que le couple (dx_0, dy_0) est solution. Soit (x, y) une autre solution. On a alors $ax + by = d$ et $adx_0 + bdy_0 = d$ et donc en faisant la différence :

$$a(x - dx_0) = -b(y - dy_0)$$

On en déduit que a divise $b(y - dy_0)$ et comme il est premier avec b, il divise $y - dy_0$. Ainsi, il existe un entier k tel que $y = dy_0 + ka$. Finalement, en reportant dans l'équation de départ, on arrive à $x = dx_0 - kb$.

Réciproquement on vérifie que x et y ainsi définis constituent bien une solution pour tout entier relatif k. Finalement, les solutions sont les couples $(dx_0 - kb, dy_0 + ka)$ pour k entier relatif. √

Remarque. Résoudre en entiers l'équation $ax + by = d$ revient géométriquement à trouver les points à coordonnées entières sur la droite d'équation cartésienne $ax + by = d$.

De façon plus anecdotique, on peut chercher à résoudre l'équation $ax+by = d$ en nombres entiers naturels. On a, dans ce sens, la proposition suivante :

Proposition 2.4.4 (Coin exchange problem of Frobenius[4]) *Soient a et b deux entiers strictement positifs et premiers entre eux. Le nombre relatif d peut s'écrire sous la forme $ax + by$ pour des entiers x et y positifs ou nuls si et seulement si le nombre $ab - a - b - x$ ne peut pas s'écrire sous cette forme.*

En particulier, $ab - a - b$ est le plus grand entier qui ne puisse pas s'écrire $ax + by$ où x et y sont des entiers positifs ou nuls.

Démonstration. Notons x_0 et y_0 des entiers tels que $ax_0+by_0=1$. On a vu dans l'exercice précédent que les solutions (en entiers relatifs) de l'équation $ax+by=d$ sont $x=dx_0-kb$ et $y=dy_0+ka$. Ainsi, l'équation admet une solution en nombre entiers positifs ou nuls si et seulement s'il existe un entier k tel que $dx_0-kb>-1$ et $dy_0+ka>-1$, autrement dit si et seulement s'il y a un entier dans l'intervalle $\left]-\frac{dy_0+1}{a}, \frac{dx_0+1}{b}\right[$.

Il s'agit donc de prouver qu'il y a un entier dans l'intervalle $\left]-\frac{dy_0+1}{a}, \frac{dx_0+1}{b}\right[$ si et seulement s'il n'y en a pas dans l'intervalle $\left]-\frac{(D-d)y_0+1}{a}, \frac{(D-d)x_0+1}{b}\right[$ où on pose $D=ab-a-b$. Or, si n est un entier, les propriétés suivantes sont équivalentes :

$$-\frac{(D-d)y_0+1}{a} < n < \frac{(D-d)x_0+1}{b}$$
$$-by_0+y_0+\frac{by_0}{a}+\frac{dy_0}{a}-\frac{1}{a} < n < ax_0-x_0-\frac{ax_0}{b}-\frac{dx_0}{b}+\frac{1}{b}$$

En se rappelant que $ax_0+by_0=1$, l'inéquation précédente se simplifie considérablement et devient :

$$-by_0+\frac{dy_0}{a} < n+x_0-y_0 < ax_0-\frac{dx_0}{b}$$

ou encore :

$$\frac{dy_0}{a} < n+x_0-y_0+by_0 < 1-\frac{dx_0}{b}$$

puis, en passant aux opposés :

$$\frac{dx_0}{b}-1 < -n-x_0+y_0-by_0 < -\frac{dy_0}{a}$$

Désormais, il suffit donc de montrer qu'il y a un entier dans l'intervalle $\left]-\frac{dy_0+1}{a}, \frac{dx_0+1}{b}\right[$ si et seulement s'il n'y en a pas dans l'intervalle $\left]\frac{dx_0}{b}-1, -\frac{dy_0}{a}\right[$.

Déjà, on remarque que le premier intervalle n'est jamais vide, puisque l'on a bien :

$$\frac{dx_0+1}{b}+\frac{dy_0+1}{a}=\frac{d+a+b}{ab}>0$$

Le second intervalle peut être vide. En effet :

$$-\frac{dy_0}{a}-\frac{dx_0}{b}+1=1-\frac{d}{ab}$$

qui peut être négatif si $d \geqslant ab$. Seulement dans ce cas, le premier intervalle est d'amplitude strictement supérieure à 1 et donc contient forcément un entier : l'équivalence est donc bien vérifiée.

Sinon, on remarque que l'intersection de deux intervalles consiste en l'intervalle $\left]-\frac{dy_0+1}{a}, -\frac{dy_0}{a}\right[$ qui ne peut contenir aucun entier, et que par contre la réunion consiste en l'intervalle $\left]\frac{dx_0}{b}-1, \frac{dx_0+1}{b}\right[$ qui contient autant d'entiers que $\left]\frac{dx_0}{b}-1, \frac{dx_0}{b}\right]$, c'est-à-dire un et un seul. Ceci démontre la proposition. □

<u>*Exercice*</u> : Soient a et b des entiers strictement positifs et premiers entre eux. Montrer que le nombre d'entiers positifs qui ne peuvent pas se mettre sous la forme $ax+by$ pour des entiers positifs ou nuls x et y est donné par la formule :

$$\frac{(a-1)(b-1)}{2}$$

Solution : D'après la proposition précédente tous les nombres strictement supérieurs à $d = ab - a - b$ peuvent se mettre sous la forme de l'énoncé. D'autre part si $n \in \{0, \ldots, d\}$, on sait que n peut se mettre sous la forme en question si, et seulement si $d - n$ ne le peut pas. Or l'application $n \mapsto d - n$ réalise une bijection de l'ensemble $\{0, \ldots, d\}$ sur lui-même. On en déduit qu'exactement la moitié des nombres de cet ensemble s'écrivent sous la forme voulue. Cela e fait $\frac{d+1}{2}$, soit encore la formule donnée dans l'énoncé. $\surd$

2.5 Exercices

Exercice 73 (Théorème de Anning) Montrer que la valeur de la fraction $\frac{101010101}{110010011}$ dont le numérateur et le dénominateur sont écrits en base b ne change pas si on remplace le 1 central du numérateur et du dénominateur par un nombre impair quelconque de 1.

Exercice 74 Montrer que tout entier naturel n peut s'écrire de façon unique sous la forme :

$$n = a_1 1! + a_2 2! + a_3 3! + \cdots + a_d d! + \cdots$$

où $a_1, a_2, a_3, \cdots$ sont des entiers tels que $0 \leqslant a_i \leqslant i$ pour tout i.

Exercice 75 Soit $a_1 > a_2 > 0$ des entiers. L'algorithme d'Euclide fournit une suite d'entiers :

$$a_1, a_2, a_3, \ldots, a_{n-1}, a_n, 0$$

où l'on rappelle que a_{i+1} est défini comme le reste de la division euclidienne de a_i par a_{i-1} et le dernier reste non nul a_n est le PGCD de a_1 et a_2.

Montrer que l'entier n vérifie l'inégalité $F_{n-1} \leqslant a_2$ où (F_n) est la suite de *Fibonacci* définie par $F_0 = 0$, $F_1 = 1$ et $F_n = F_{n-1} + F_{n-2}$ pour $n \geqslant 2$.

Exercice 76 Trouver tous les entiers a, b et c vérifiant l'équation $5a + 3b + 15c = 2$.

Exercice 77 (Canada 85) Trouver tous les entiers n tels que 2^{n-1} divise $n!$.

Exercice 78* (Yougoslavie 99) Soit $n > 0$ un entier. On note s_n la somme des chiffres de l'écritrure décimale de n. Existe-t-il un entier $n > 0$ tel que $s(n) = 1997$ et $s(n^2) = 1997^2$?

Exercice 79* On note $\varphi(n)$ le nombre d'entiers positifs inférieurs à n et premiers avec n. Montrer que si $n > 2$, $\varphi(n)$ est toujours pair.

Exercice 80* (Allemagne 95) Dans le plan, un jeton est déplacé selon les règles suivantes ;

i) De tout point (a, b), on peut le déplacer en $(a, 2b)$ ou $(2a, b)$;

ii) De tout point (a, b) avec $a > b$, on peut le déplacer en $(a - b, b)$. Et si $a < b$, on peut le déplacer en $(a, b - a)$.

Le jeton est initialement en $(1, 1)$. Déterminer une condition nécessaire et suffisante sur x et y pour que l'on puisse amener le jeton en (x, y) en un nombre fini d'étapes.

Exercice 81* Pour tout n strictement positif, on note $P(n)$ le produit des chiffres non nuls de l'écriture de n en base 10. Un entier n est dit *prodigieux* lorsque $P(n)$ divise n. Prouver qu'il n'existe pas 14 entiers consécutifs qui soient tous prodigieux.

Exercice 82* (Hollande 04) Soit (u_n) une suite d'entiers vérifiant $u_1 = 2$, $u_2 = 3$ et $u_{n+1} = 2u_{n-1}$ ou $u_{n+1} = 3u_n - 2u_{n-1}$ pour tout $n \geqslant 2$. Montrer que pour tout n, l'entier u_n a au plus deux chiffres non nuls en base 2.

Exercice 83* (Roumanie 97) Soient $n \geqslant 3$ un entier et x un réel positif ou nul. Prouver que les nombres x, x^2, x^n ont la même partie décimale si, et seulement si x est un entier.

Exercice 84* (URSS 71) Démontrer que pour tout entier $n > 0$ il existe un nombre dont l'écriture décimale n'utilise que des 1 et des 2, et qui est divisible par 2^n.

Exercice 85* (URSS 89) a) Soient a et b des réels distincts tels que, pour tout entier naturel n, le nombre $a^n - b^n$ soit entier. Les nombres a et b sont-ils rationnels ? Sont-ils entiers ?

b) Existe-t-il des réels distincts a et b pour lesquels le nombre $a + b$ est rationnel alors que $a^n + b^n$ est irrationnel pour tout entier $n \geqslant 2$?

c) Existe-t-il des réels distincts a et b pour lesquel le nombre $a + b$ est irrationnel alors que $a^n + b^n$ est rationnel pour tout entier $n \geqslant 2$?

Exercice 86* (Devinette) Les martiens sont un peu bizarres quand même. Ma voisine par exemple en est une. Outre le fait qu'elle ait six doigts à chaque main, j'ai l'impression qu'elle écrit des inepties sous son cahier de maths. Par l'exemple, l'autre jour, j'ai vu la formule :

$$(5x + 3)(3x - 7) = 13x^2 - 22x - 19$$

Pouvez-vous m'aider à comprendre, car j'ai entendu dire qu'elle était très forte en maths, et ne se trompait jamais en calcul ?

Exercice 87* (Problem of the month – Regina) La suite S de Kolakoski :

$$1, 2, 2, 1, 1, 2, 1, 2, 2, 1, 2, 2, \ldots$$

est un exemple de suite « qui se lit elle-même ». Elle est constituée de groupes de 1 et de groupes de 2 en alternance, la longueur du n-ième groupe étant la valeur du n-ième terme de la suite.

Prouver que le nombre $x = 0,122\,112\,122\,122\ \ldots$ est irrationnel.

Exercice 88* (OIM 85) Soit n un entier naturel, k un entier premier avec n, $1 \leqslant k \leqslant n-1$, M l'ensemble $\{1, 2, \ldots, n-1\}$. Chaque élément de M est coloré avec l'une des deux couleurs blanche ou bleue. On suppose :

(1) pour tout i de M, i et $n - i$ ont la même couleur,

(2) pour tout i de M, $i \neq k$, i et $|i - k|$ ont la même couleur.

Montrer que tous les éléments de M ont la même couleur.

Exercice 89* (Japon 96) Soient m et n des entiers premiers entre eux. Calculer le PGCD des entiers $5^m + 7^m$ et $5^n + 7^n$.

Exercice 90* Soit $p_1, p_2, \ldots, p_n, \ldots$ la suite des nombres premiers. Montrer que le nombre dont l'écriture décimale est :

$$0, p_1 p_2 p_3 \ldots p_n \ldots$$

est irrationnel.

Exercice 91* Trouver tous les entiers $n > 1$ pour lesquels la somme $2^2 + 3^2 + \cdots + n^2$ est une puissance d'un nombre premier.

Exercice 92* Dans ma boîte de céréales, j'ai trouvé le jeu suivant. Il se compose des six cartes que je reproduis ci-dessous.

1	3	5	7
9	11	13	15
17	19	21	23
25	27	29	31
33	35	37	39
41	43	45	47
49	51	53	55
57	59	61	63

2	3	6	7
10	11	14	15
18	19	22	23
26	27	30	31
34	35	38	39
42	43	46	47
50	51	54	55
58	59	62	63

4	5	6	7
12	13	14	15
20	21	22	23
28	29	30	31
36	37	38	39
44	45	46	47
52	53	54	55
60	61	62	63

8	9	10	11
12	13	14	15
24	25	26	27
28	29	30	31
40	41	42	43
44	45	46	47
56	57	58	59
60	61	62	63

16	17	18	19
20	21	22	23
24	25	26	27
28	29	30	31
48	49	50	51
52	53	54	55
56	57	58	59
60	61	62	63

32	33	34	35
36	37	38	39
40	41	42	43
44	45	46	47
48	49	50	51
52	53	54	55
56	57	58	59
60	61	62	63

Pour jouer, je dois demander à un partenaire de penser secrètement à un nombre compris entre 1 et 63, puis de me montrer les cartes sur lequel son nombre apparaît. Normalement, je suis supposé savoir retrouver le nombre choisi avec ces seules informations, mais la partie qui explique cette déduction a été déchirée lors de l'ouverture de la boîte.

Peux-tu m'aider à retrouver comment on fait ?

Exercice 93* Soit A l'ensemble des entiers strictement positifs dont l'écriture en base 3 n'utilise pas le chiffre 2. Montrer que trois éléments de A ne sont jamais en progression arithmétique.

Exercice 94* Trouver tous les entiers $a > 0$ et $b > 2$ tel que $2^a + 1$ soit un multiple de $2^b - 1$.

Exercice 95* Soit P un polynôme à coefficients entiers. On définit la suite (a_n) en posant $a_0 = 0$ et $a_{i+1} = P(a_i)$ pour tout $i \geqslant 0$. Montrer que :

$$\text{PGCD}(a_m, a_n) = a_{\text{PGCD}(m,n)}$$

Exercice 96* (Entiers de Gauss) On note :

$$\mathbf{Z}[i] = \{x + iy,\ x, y \in \mathbf{Z}\}$$

Soient $a, b \in \mathbf{Z}[i]$ avec $b \neq 0$. Montrer qu'il existe des éléments q et r dans $\mathbf{Z}[i]$ tels que $a = bq + r$ et $|r| < |b|$. Cette écriture est-elle unique ?

Exercice 97* (Ibéroamérique 94) Un entier $n > 0$ est dit *brésilien* s'il existe $r < n - 1$ pour lequel n s'écrit en base r avec des chiffres tous égaux. Montrer que 1994 est brésilien mais que 1993 ne l'est pas.

Exercice 98* (Crux Mathematicorum) Soit $k \geqslant 2$ un entier fixé. Pour tout entier $n \geqslant 0$, on désigne par x_n le chiffre de gauche dans l'écriture décimale du nombre n^k. Prouver que le nombre :

$$0, x_0 x_1 x_2 \dots x_n \dots$$

est irrationnel.

Exercice 99* (APMO 94) Dans le première colonne (resp. deuxième colonne) du tableau ci-dessous, on écrit les nombres 10^k en base 2 (resp. en base 5).

1010	20
1100100	400
1111101000	13000
⋮	⋮

Soit $n > 1$ un entier. Prouver qu'il apparaît dans le tableau précédent un et un unique nombre de n chiffres.

Exercice 100* (Problem of the month – Regina) Déterminer tous les couples (d, n) d'entiers strictement positifs tels que d divise n et $nd + 1$ divise $n^2 + d^2$.

Exercice 101* (URSS 65) Soit $n > 0$ un entier. Prouver que tout entier inférieur ou égal à $n!$ peut s'écrire comme la somme d'au plus n diviseurs de $n!$ deux à deux distincts.

Exercice 102 (OIM 91)** Soient $n > 6$ un entier et $a_1, \dots, a_k$ tous les entiers compris strictement entre 0 et n qui sont premiers avec n. On suppose :

$$a_2 - a_1 = a_3 - a_2 = \dots = a_k - a_{k-1} > 0$$

Montrer que n est soit un nombre premier, soit une puissance entière de 2.

Exercice 103** On définit la suite (a_n) par $a_1 = 2$, $a_{n+1} = \left[\frac{3}{2} a_n\right]$. Montrer que a_n est pair (resp. impair) pour une infinité de valeurs de n.

Exercice 104 (Russie 01)** Déterminer tous les entiers $n > 1$ tels que, pour tous diviseurs a et b de n premiers entre eux, le nombre $a + b - 1$ est aussi un diviseur de n.

Exercice 105 (Slovénie 99)** Trois boîtes contiennent chacune au moins un jeton. Une opération consiste à choisir deux boîtes et à transvaser des jetons de l'une à l'autre de façon

à doubler le nombre de jetons dans la boîte d'arrivée. Est-il possible de vider l'une des boîtes en un nombre fini d'opérations ?

Exercice 106** Soit $x_0 \in [0,1]$. On définit la suite x_n par $x_{n+1} = 1 - |1 - 2x_n|$. Montrer que (x_n) est périodique à partir d'un certain rang si, et seulement si x_0 est rationnel.

Exercice 107** La suite de *Fibonacci* est définie par $F_0 = 0$, $F_1 = 1$ et $F_n = F_{n-1} + F_{n-2}$ pour $n \geqslant 2$.

a) Montrer que $F_{n+p} = F_{p-1}F_n + F_{n+1}F_p$ pour tous n et p.

b) Montrer en utilisant la formule précédente que si $d = \text{PGCD}\,(m,n)$, alors $\text{PGCD}\,(F_m, F_n) = F_d$

Exercice 108 (Pologne 96)** Pour tout entier k strictement positif, on désigne par $p\,(k)$ le plus petit nombre premier ne divisant pas k, et par $q\,(k)$ le produit de tous les nombres premiers strictement inférieurs à $p\,(k)$ (si $p\,(k) = 2$, on convient que $q\,(k) = 1$).

On définit une suite en posant $x_0 = 1$ et $x_{n+1} = x_n \frac{p(x_n)}{q(x_n)}$. Déterminer les entiers n pour lesquels $x_n = 111111$.

Exercice 109* (OIM 88)** On désigne par f l'application de $\mathbf{N}^\star$ dans lui-même définie par :

$$f\,(1) = 1, \quad f\,(3) = 3$$

et pour tout $n \geqslant 1$:

$$\begin{aligned} f\,(2n) &= f\,(n) \\ f\,(4n+1) &= 2f\,(2n+1) - f\,(n) \\ f\,(4n+3) &= 3f\,(2n+1) - 2f\,(n) \end{aligned}$$

Déterminer le nombre d'entiers n, $1 \leqslant n \leqslant 1988$, pour lesquels $f\,(n) = n$.

Exercice 110* (Lituanie 94)** Si N est un entier, on note $S\,(N)$ la somme des chiffres (en base 10) de N. Montrer que la suite $S\,(2^n)$ tend vers l'infini.

3 Congruences

3.1 Définition, premières propriétés

Tout un chacun sait que l'on peut répartir les entiers en deux catégories : les nombres pairs, et les nombres impairs. Et que cette répartition est compatible avec les opérations ; par exemple, la somme d'un nombre pair et d'un nombre impair est impaire, le produit d'un nombre pair et d'un nombre impair est pair, etc. En fait, cela est souvent bien pratique. Les congruences généralisent ce type de raisonnement.

Définition 3.1.1 Soit $N > 1$ un entier. Deux entiers a et b sont dits *congrus modulo* N lorsque N divise $b - a$ (ou de façon équivalente $a - b$). On note $a \equiv b \pmod N$.

La relation de congruence vérifie les propriétés suivantes (immédiates) :

Propriétés

- ☞ On a $a \equiv 0 \pmod N$ si, et seulement si N divise a.
- ☞ Si $a \equiv b \pmod N$ et $b \equiv c \pmod N$, alors $a \equiv c \pmod N$.
- ☞ On a $a \equiv b \pmod{N_1}$ et $a \equiv b \pmod{N_2}$ si, et seulement si $a \equiv b \pmod{\text{PPCM}(N_1, N_2)}$.
- ☞ Tout entier est congru modulo N à un et un unique élément de l'ensemble $\{0, \ldots, N-1\}$. Il s'agit précisément du reste de la division euclidienne de cet entier par N. On dit parfois que l'ensemble $\{0, \ldots, N-1\}$ est un *système complet de résidus* modulo N. Un élément d'un système complet de résidu modulo N est parfois appelé un *résidu*.
- ☞ Les entiers congrus à a modulo N sont les entiers de la forme $a + kN$, avec k entier.
- ☞ Si $a \equiv b \pmod N$ et $a' \equiv b' \pmod N$, alors $a + a' \equiv b + b' \pmod N$ et $aa' \equiv bb' \pmod N$.

Malgré l'évidence apparente des propriétés précédentes, elles s'avèrent vraiment très utiles à toutes sortes de moments. Par exemple la finitude d'un système complet de résidus permet, lorsque l'on a une équation à résoudre faisant intervenir des congruences dont le modulo est un entier connu, de ne tester qu'un nombre fini de cas. Souvent, il y a des astuces mais il ne faut jamais désespérer si on n'en trouve pas. Par exemple, en testant tous les cas, on prouve facilement que le carré d'un entier est toujours congru à 0 ou 1 modulo 4. De même une étude exhaustive peut permettre de résoudre la question suivante :

Exercice : Trouver tous les entiers x tels que 7 divise $x^2 + x + 1$.

Solution : La condition se réécrit $x^2 + x + 1 \equiv 0 \pmod 7$. En essayant les sept résidus, on voit que les seules solutions sont les entiers congrus à 2 ou 4 modulo 7. √

Théorème 3.1.2 *Soit $N > 1$ un entier et c un entier premier avec N. Alors il existe un entier c' tel que $cc' \equiv 1 \pmod N$.*

Un tel entier c' est appelé un inverse *de c modulo N.*

Démonstration. Il s'agit d'une simple application du théorème de Bézout. Comme N et c sont premiers entre eux, on peut écrire une égalité du type $uN + vc = 1$. On voit directement que l'entier $c' = v$ convient pour le théorème.

On remarque également que l'algorithme d'Euclide étendu donne un moyen effectif pour calculer l'inverse de c modulo N. □

Remarque. L'implication donnée dans le théorème précédent est en réalité une équivalence : si c admet un inverse modulo N, alors c est premier avec N. En effet, dire que c admet un inverse modulo N signifie qu'il existe des entiers k et c' tels que $cc' = 1 + kN$. Le sens facile du théorème de Bézout permet de conclure.

Si c' est un inverse de c modulo N et que le contexte ne prête pas à confusion, il arrive que l'on note $c' = c^{-1}$, voire $c' = \frac{1}{c}$. En particulier, si q est un entier premier avec N, la fraction $\frac{p}{q}$ pourra désigner un résidu modulo N.

Le théorème précédent n'est en réalité qu'une reformulation du théorème de Bézout comme le montre la preuve précédente. Il a une conséquence importante qui est la traduction en termes de congruences du lemme de Gauss :

Proposition 3.1.3 *Soient $N > 1$ un entier et a, b et c des entiers tels que $ac \equiv bc \pmod N$. Si c est premier avec N, alors on peut déduire que $a \equiv b \pmod N$.*

Démonstration. Comme c est premier avec N, il admet un inverse modulo N, disons c'. En multipliant par c' la congruence $ac \equiv bc \pmod N$, on obtient directement le résultat. □

Remarque. Si c n'est pas premier avec N, on a simplement une conclusion plus faible qui est :

$$a \equiv b \pmod{\frac{N}{\text{PGCD}\,(c, N)}}$$

On remarquera même que cette dernière congruence est équivalente à $ac \equiv bc \pmod N$. On laisse la démonstration de cette équivalence au lecteur.

3.2 Critères de divisibilité

Les critères de divisibilité que l'on apprend dans les petites classes trouvent leur justification dans des manipulations simples de congruences. Supposons pour cela que l'on dispose d'un entier n s'écrivant $n_d n_{d-1} \cdots n_0$ en base 10, c'est-à-dire tel que l'on ait :

$$n = 10^d n_d + 10^{d-1} n_{d-1} + \cdots 10 n_1 + n_0$$

On voit directement sur cette écriture que l'on a toujours $n \equiv n_0 \pmod{10}$. De même en regardant modulo 2 et modulo 5, on obtient les critères de divisibilité bien connus suivants :

Critères de divisibilité

- ☞ Un entier est divisible par 10 si, et seulement s'il se termine par un 0.
- ☞ Un entier est divisible par 5 si, et seulement s'il se termine par un 0 ou par un 5.
- ☞ Un entier est divisible par 2 si, et seulement s'il se termine par un 0, un 2, un 4, un 6 ou un 8.

Bien évidemment, ces critères admettent un analogue (dont le démonstration est rigoureusement identique) pour une base b quelconque :

Théorème 3.2.1 *Soit $b \geqslant 2$ un entier et d un diviseur de b. Alors un entier est divisible par d si, et seulement si le dernier chiffre de son écriture en base b est lui-même divisible par d.*

De même il est possible de retrouver les critères de divisibilité classiques par 3 et 9. En effet, si N désigne l'un des deux entiers 3 ou 9, on a $10 \equiv 1 \pmod N$ et donc la congruence :

$$n \equiv n_d + n_{d-1} + \cdots n_1 + n_0 \pmod N$$

qui prouve :

Critères de divisibilité

- ☞ Un entier est divisible par 9 si, et seulement si la somme de ses chiffres l'est.
- ☞ Un entier est divisible par 3 si, et seulement si la somme de ses chiffres l'est.

De même, ces critères se généralisent à une base quelconque :

Théorème 3.2.2 *Soit $b \geqslant 2$ un entier et d un diviseur de $b-1$. Alors un entier est divisible par d si, et seulement si la somme des chiffres de son écriture en base b est elle-même divisible par d.*

Il est possible d'inventer d'autres critères à perte de vue. Par exemple en remarquant que $100 \equiv 0 \pmod 4$ ou que $10 \equiv -1 \pmod{11}$, on obtient les deux critères suivants :

Critères de divisibilité

- ☞ Un entier est divisible par 4 si, et seulement si le nombre formé par ses deux derniers chiffres (en base 10) l'est.
- ☞ Un entier est divisible par 11 si, et seulement si la somme des ses chiffres (en base 10) de rang pair diminuée de la somme de ses chiffres de rang impair est divisible par 11.

Le lecteur amusé pourra inventer sur le même principe multitude de nouveaux critères de divisibilité. Ceux-ci, cependant, sont en général peu utiles en pratique.

3.3 Ordre d'un élément

Fixons un entier $N > 1$ et a un entier premier avec N. Comme il n'y a que N résidus modulo n, il existe des entiers s et t avec $s < t$ tels que $a^s \equiv a^t \pmod N$. Comme a est premier avec N, il admet un inverse a' modulo N. En multipliant la congruence précédente par a'^s, on obtient $a^{t-s} \equiv 1 \pmod N$. On peut donc poser la définition suivante :

Définition 3.3.1 Soit a un entier premier avec N. On appelle *ordre* de a modulo N, le plus petit entier $k > 0$ tel que $a^k \equiv 1 \pmod N$.

Remarque. Si a n'est pas premier avec N, il n'admet pas d'ordre modulo N. Autrement dit, il n'existe aucun entier $k > 0$ tel que $a^k \equiv 1 \pmod N$. En effet, cette dernière congruence impliquerait que a^{k-1} est un inverse de a modulo N, ce qui n'existe pas.

La notion d'ordre est souvent des plus utiles. Voyons tout de suite une première façon de s'en servir :

Exercice : Si n est un entier premier avec 10, il possède un multiple qui ne s'écrit qu'avec des chiffres 1.

Solution : On remarque que $1\dots1$ (k fois) vaut $\frac{10^k-1}{9}$. Comme 10 est premier avec n, il l'est aussi avec $9n$. Notons k l'ordre de 10 modulo $9n$. Alors $9n$ divise 10^k-1, et finalement, l'entier $\frac{10^k-1}{9}$ est un multiple de n dont l'écriture en base 10 ne comporte que des 1. $\surd$

Il est facile mais intéressant de remarquer que si a est premier avec N et si k désigne l'ordre de a modulo N, alors $a^{n+k} \equiv a^n \pmod N$ pour tout n. On dit que la suite des a^n est *périodique* modulo N. Par définition, l'ordre correspond exactement à la période de cette suite. Autrement dit, on a la proposition suivante dont il ne faut pas négliger l'utilité :

Proposition 3.3.2 *Avec les notations précédentes, si n vérifie $a^n \equiv 1 \pmod N$, alors il est divisible par k (l'ordre de a modulo N).*

3.4 Théorème chinois

Le théorème chinois s'énonce comme suit :

Théorème 3.4.1 *Soient $N_1, N_2, \dots, N_k$ des entiers strictement positifs deux à deux premiers entre eux, et $a_1, a_2, \dots, a_k$ des entiers quelconques. Alors il existe un entier a tel que le système de congruences :*

$$\left\{\begin{array}{lcll} x & \equiv & a_1 & \pmod{N_1} \\ x & \equiv & a_2 & \pmod{N_2} \\ & \vdots & & \\ x & \equiv & a_k & \pmod{N_k} \end{array}\right.$$

soit équivalent à la simple congruence $x \equiv a \pmod{N_1 N_2 \cdots N_k}$.

En particulier, le système précédent possède au moins une solution.

Démonstration. On remarque dans un premier temps qu'il suffit de prouver le théorème lorsque $k=2$. Une récurrence directe permettra ensuite de l'avoir dans toute sa généralité.

On cherche à résoudre l'équation $x \equiv a_1 \pmod{N_1}$ et $x \equiv a_2 \pmod{N_2}$. La première condition assure l'existence d'un entier q tel que $x = a_1 + qN_1$ et la seconde congruence s'écrit alors :

$$a_1 + N_1 q \equiv a_2 \pmod{N_2}$$

ce qui fournit :

$$q \equiv (a_2 - a_1)\, N_1' \pmod{N_2}$$

où N_1' désigne un inverse de N_1 modulo N_2 qui existe bien car N_1 et N_2 sont supposés premiers entre eux. Ainsi si l'on pose $a = a_1 + (a_2 - a_1)\, N_1' N_1$, on obtient $x \equiv a \pmod{N_1 N_2}$.

La réciproque est immédiate. $\square$

Remarque. La démonstration précédente fournit en réalité (*via* l'algorithme d'Euclide étendu) un moyen effectif de calculer l'entier a du théorème.

Le théorème chinois est utile principalement dans deux situations. La première se présente lorsque l'on demande de construire un entier vérifiant un certain nombre de conditions arithmétiques. Si l'on arrive ainsi à traduire ces conditions en terme de congruence (ou plus modestement à trouver des conditions plus faibles qui s'expriment en terme de congruence), on pourra appliquer le théorème précédent pour résoudre la question. Un exemple classique est donné par l'exercice suivant :

Exercice : Prouver qu'il existe n nombres consécutifs qui ne sont pas des puissances parfaites (*i.e.* ne s'écrivent pas sous la forme a^k pour des entiers a et k avec $k > 1$).

Solution : On remarque que si p est un nombre premier et si $x \equiv p \pmod{p^2}$, alors x ne peut pas être une puissance parfaite puisque $v_p(x) = 1$ forcément.

Désignons par $p_1, \dots, p_n$ des nombres premiers deux à deux distincts et intéressons-nous au système suivant :

$$\left\{\begin{array}{lll} x & \equiv & p_1 - 1 \pmod{p_1^2} \\ x & \equiv & p_2 - 2 \pmod{p_2^2} \\ & \vdots & \\ x & \equiv & p_n - n \pmod{p_n^2} \end{array}\right.$$

Puisque les p_i^2 sont premiers entre eux, d'après le théorème chinois il existe une solution à ce système. Et si x est solution, alors $x + i \equiv p_i \pmod{p_i^2}$ et donc n'est pas une puissance parfaite. Cela conclut. $\surd$

Remarque. La difficulté dans cet exercice consiste à transformer la condition de l'énoncé en condition de congruence. Souvent pour cela, il est nécessaire de faire preuve d'originalité... mais certains réflexes doivent survenir, comme celui de considérer la suite des nombres premiers.

La seconde situation se présente lorsque l'on est amené à considérer des congruences modulo un entier N. Nous allons voir dans les paragraphes suivants que l'étude des congruences modulo N est plus facile lorsque N est un nombre premier ou une puissance d'un nombre premier (en effet, on dispose de plus de théorèmes dans ces cas). Ainsi, il peut être intéressant de décomposer N en facteurs premiers :

$$N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

et à considérer la congruence modulo chacun des $p_i^{\alpha_i}$. Le théorème chinois permet alors de tout remettre ensemble.

Notons finalement qu'il existe une généralisation (moins connue) du lemme chinois dans le cas où les modulos ne sont pas premiers entre eux :

Proposition 3.4.2 *Soient $N_1, N_2, \dots, N_k$ des entiers strictement positifs, et $a_1, a_2, \dots, a_k$ des entiers quelconques. Alors le système suivant :*

$$(S) : \left\{\begin{array}{lll} x & \equiv & a_1 \pmod{N_1} \\ x & \equiv & a_2 \pmod{N_2} \\ & \vdots & \\ x & \equiv & a_k \pmod{N_k} \end{array}\right.$$

admet une solution si, et seulement si pour tous i et j, on a $a_i \equiv a_j \pmod{\text{PGCD}(N_i, N_j)}$. Dans le cas où (S) admet une solution, il existe un entier a tel que (S) soit équivalent à la seule congruence :

$$x \equiv a \pmod{\text{PPCM}(N_1, N_2, \dots, N_k)}$$

Démonstration. Supposons dans un premier temps que le système admette une solution x. Soient i et j deux indices. On a $x \equiv a_i \pmod{N_i}$ et donc *a fortiori*, on a $x \equiv a_i \pmod{\text{PGCD}(N_i, N_j)}$. De même, on obtient $x \equiv a_j \pmod{\text{PGCD}(N_i, N_j)}$, d'où on déduit $a_1 \equiv a_2 \pmod{\text{PGCD}(N_i, N_j)}$.

Faisons la réciproque. On raisonne pour cela par récurrence. Commençons donc par traiter le cas $k = 2$. Posons pour cela $x' = x - a_1$. Le système est alors équivalent à :

$$\begin{cases} x' \equiv 0 \pmod{N_1} \\ x' \equiv a_2 - a_1 \pmod{N_2} \end{cases}$$

avec $a_1 \equiv a_2 \pmod d$ où on a posé $d = \text{PGCD}(N_1, N_2)$. Une solution x' est alors forcément un multiple de N_1 et donc un multiple de d. En posant $x'' = \frac{x'}{d}$, le système devient équivalent à :

$$\begin{cases} x'' \equiv 0 \pmod{\frac{N_1}{d}} \\ x'' \equiv \frac{a_2 - a_1}{d} \pmod{\frac{N_2}{d}} \end{cases}$$

Les entiers $\frac{N_1}{d}$ et $\frac{N_2}{d}$ sont premiers entre eux. On peut donc appliquer le théorème chinois, et en utilisant la formule :

$$\text{PGCD}(N_1, N_2)\, \text{PPCM}(N_1, N_2) = N_1 N_2$$

on obtient la conclusion voulue.

Il reste à traiter l'hérédité. Supposons donc donné le système suivant :

$$(S) : \begin{cases} x & \equiv & a_1 \pmod{N_1} \\ x & \equiv & a_2 \pmod{N_2} \\ & \vdots & \\ x & \equiv & a_k \pmod{N_k} \end{cases}$$

où l'on a les congruences $a_i \equiv a_j \pmod{\text{PGCD}(N_i, N_j)}$ pour tous i et j. Les deux premières lignes de (S) sont, d'après le cas traité précédemment, équivalentes à la seule congruence :

$$x \equiv a_{1,2} \pmod{\text{PPCM}(N_1, N_2)}$$

pour un certain entier $a_{1,2}$ forcément congru à a_1 modulo N_1 et congru à a_2 modulo N_2. Le système (S) devient donc équivalent à :

$$(S') : \begin{cases} x & \equiv & a_{1,2} \pmod{\text{PPCM}(N_1, N_2)} \\ x & \equiv & a_3 \pmod{N_3} \\ & \vdots & \\ x & \equiv & a_k \pmod{N_k} \end{cases}$$

Soit i un indice compris entre 3 et k. On a d'une part les congruences :

$$\begin{aligned} a_i &\equiv a_1 \equiv a_{1,2} \pmod{\text{PGCD}(N_i, N_1)} \\ a_i &\equiv a_2 \equiv a_{1,2} \pmod{\text{PGCD}(N_i, N_2)} \end{aligned}$$

d'où on déduit :

$$a_i \equiv a_{1,2} \pmod{\text{PPCM}(\text{PGCD}(N_i, N_1), \text{PGCD}(N_i, N_2))}$$

Mais d'autre part, on a l'égalité :

$$\text{PGCD}(N_i, \text{PPCM}(N_1, N_2)) = \text{PPCM}(\text{PGCD}(N_i, N_1), \text{PGCD}(N_i, N_2))$$

et donc finalement le système (S') vérifie l'hypothèse de récurrence. On conclut ainsi. □

3.5 Congruences modulo p

On suppose dans ce paragraphe que $N = p$ est un nombre premier et on étudie plus spécifiquement les congruences modulo p. La propriété fondamentale est la suivante : lorsque p est premier, tout nombre qui n'est pas divisible par p est premier avec p. Ainsi tous les résidus non nuls sont inversibles modulo p.

Cela implique par exemple la propriété agréable suivante :

Proposition 3.5.1 *Si a et b sont des entiers tels que $ab \equiv 0 \pmod{p}$, alors soit $a \equiv 0 \pmod{p}$, soit $b \equiv 0 \pmod{p}$*

Démonstration. Supposons que a ne soit pas un multiple de p. Alors a est premier avec p et donc il admet un inverse a'. En multipliant la congruence $ab \equiv 0 \pmod{p}$ par a', on obtient bien $b \equiv 0 \pmod{p}$. □

Remarque. Cette propriété n'est pas nouvelle : si l'on regarde bien, c'est exactement celle énoncée dans le lemme 1.2.3. Toutefois, la formulation précédente permet de la rapprocher d'une propriété analogues des nombres réels à savoir *si un produit est nul, alors l'un des facteurs est nul*. On sait que cette propriété est souvent utilisée pour résoudre des équations polynômiales de degré 2 ou supérieur... on pourra donc utiliser des méthodes analogues dans ce contexte modulo p.

Un autre fait important qui peut-être vu comme une conséquence de ce qui précède est que l'on dispose d'une estimation de l'ordre d'un élément modulo p :

Théorème 3.5.2 (Petit théorème de Fermat) *Si p est un nombre premier et a un entier non divisible p, on a $a^{p-1} \equiv 1 \pmod{p}$. Ainsi l'ordre de a est un diviseur de $p-1$.*

Démonstration. Considérons l'ensemble des résidus non nuls modulo p. La multiplication par a définit une application de cet ensemble dans lui-même. C'est une bijection puisque l'ensemble des résidus est fini et puisque si $ax \equiv ay \pmod{p}$, alors $x \equiv y \pmod{p}$. Ainsi :

$$(1a)(2a)(3a)\cdots((p-1)a) \equiv (1)(2)(3)\cdots(p-1) \pmod{p}$$

c'est-à-dire $(p-1)!a^{p-1} \equiv (p-1)! \pmod{p}$. Le facteur $(p-1)!$ est premier avec p, donc inversible modulo p et le théorème est prouvé. □

Remarque. On énonce parfois le théorème de Fermat sous la forme directement équivalente suivante : pour tout entier a, on a $a^p \equiv a \pmod{p}$. On peut se demander si les nombres premiers sont les seuls à vérifier de telles congruences pour tout entier a. La réponse est négative comme le montre l'exemple de $561 = 3 \times 11 \times 17$. Ces exemples sont rares et s'appellent les *nombres de Carmichael*.

Le résultat précédent se généralise lorsque le modulo n'est pas premier : si n un entier strictement positif et si a est un entier premier avec n, alors $a^{\varphi(n)} \equiv 1 \pmod{n}$ où $\varphi(n)$ désigne le nombre d'entiers compris entre 1 et n et premiers avec n. La fonction φ est appelée *fonction indicatrice d'Euler*. Toutefois cette formulation est souvent moins agréable car la restriction sur les entiers a est plus difficile à exploiter et l'exposant $\varphi(n)$ plus difficile à calculer.

Comme application, citons deux exercices assez proches :

<u>*Exercice*</u> : Déterminer les entiers naturels n tels que n divise $2^n - 1$.

<u>*Solution*</u> : Il est clair que $n = 1$ convient. Montrons qu'il n'existe pas d'autre solution en considérant un entier $n > 1$ tel que n divise $2^n - 1$. La condition de l'énoncé s'écrit $2^n \equiv 1 \pmod{n}$. La congruence modulo n n'est pas très aisée à manipuler, c'est pourquoi on se restreint modulo un diviseur premier p de n. On a alors $2^n \equiv 1 \pmod{p}$. Par ailleurs, le petit théorème de Fermat entraîne que l'on a $2^{p-1} \equiv 1 \pmod{p}$. Introduisons δ l'ordre de 2 modulo p : d'après ce qui précède, δ divise n et $p-1$. Mais jusqu'à présent, nous n'avons imposé aucune condition sur p : si on le choisit comme étant le plus petit diviseur premier de n, δ est strictement inférieur à p et divise n, donc $\delta = 1$ d'où p divise 1, ce qui est absurde et permet de conclure. √

<u>*Exercice*</u> : Montrer que si $n > 1$ divise $2^n + 1$, alors n est divisible par 3.

<u>*Solution*</u> : Là encore, considérons $n > 1$ tel que n divise $2^n + 1$, puis p un facteur premier de n et δ l'ordre de 2 modulo p. La condition imposée sur n entraîne $2^n \equiv -1 \pmod{p}$, d'où $2^{2n} \equiv 1 \pmod{p}$ et δ divise $2n$ et $p-1$. Si on a pris p comme étant le plus petit facteur premier de n, on a donc $\delta = 1$ ou $\delta = 2$. Le premier cas étant exclu, $2^2 \equiv 1 \pmod{p}$ donc $p = 3$. √

Remarque. Les deux exemples précédents montrent bien que quitte à considérer un diviseur premier de n, on peut ajouter une condition de minimalité pour le même prix.

Il n'est pas possible de conclure ce chapitre sans citer le théorème de Wilson, rarement utile à vrai dire, mais devant faire partie du bagage culturel :

Théorème 3.5.3 (Wilson) *Soit $N > 1$ un entier. La congruence $(N-1)! \equiv -1 \pmod{N}$ a lieu si et seulement si N est premier.*

Démonstration. Supposons N composé. On distingue deux cas.

Si $N = p^2$, on a :

$$v_p((p^2-1)!) \geqslant \left[\frac{p^2-1}{p}\right] = p-1$$

Si $p \geqslant 2$, le nombre $(p^2-1)!$ est multiple de p^2 est donc non congru à -1 modulo p^2. On vérifie que c'est également le cas pour $p = 2$.

Sinon N n'est pas le carré d'un nombre premier, on peut écrire $N = ab$ pour deux nombres a et b inférieurs ou égaux à $N-1$ et *distincts*. On voit alors que N divise $(N-1)!$ et on conclut comme précédemment.

Si maintenant $N = p$ est premier, on constate que l'on peut regrouper les résidus non nuls modulo p deux à deux en associant chacun avec son inverse. Seuls 1 et -1 vont rester seuls. Le produit de tous les résidus sera donc égal à 1 multiplié par -1 multiplié par un certain nombre de fois 1, ce qui fait bien -1. □

3.6 Congruences modulo p^n

La notation p désigne encore un nombre premier, et n désigne un entier quelconque supérieur ou égal à 1. Le résultat principal de ce chapitre est le lemme de Hensel qui permet de remonter modulo p^n les solutions modulo p de certaines équations. Plus précisément, nous avons :

Théorème 3.6.1 (Lemme de Hensel) *Soient des entiers $a_0, a_1, \ldots, a_k$ des entiers. On définit le polynôme P par la formule :*

$$P(X) = a_0 + a_1 X + \cdots + a_k X^k$$

et le polynôme dérivé de P par la formule :

$$P'(X) = a_1 + 2a_2 X + \cdots + k a_k X^{k-1}$$

Soit x_1 un entier tel que $P(x_1) \equiv 0 \pmod p$ et $P'(x_1) \not\equiv 0 \pmod p$. Alors il existe un entier x tel que $P(x) \equiv 0 \pmod{p^n}$ et $x \equiv x_1 \pmod p$.

De plus si x et x' vérifient les deux conditions précédentes, on a $x \equiv x' \pmod{p^n}$.

Remarque. On dit souvent que la solution x_1 modulo p se *relève* en une solution x modulo p^n. La deuxième partie du théorème dit en substance que ce relèvement est unique.

Démonstration. On aura besoin pour cette démonstration de la congruence suivante :

$$(x+y)^j \equiv x^j + jx^{j-1}y \pmod{y^2}$$

qui est une conséquence immédiate de la formule du binôme de Newton rappelée dans le paragraphe 3.7.

Prouvons l'existence, c'est-à-dire la première partie du théorème. On procède par récurrence en construisant une suite d'entiers x_i tels que $x_i \equiv x_1 \pmod p$ et $P(x_i) \equiv 0 \pmod{p^i}$. Pour conclure il suffira de prendre $x = x_n$. L'entier x_1 est donné par hypothèse et permet d'initialiser la récurrence.

Supposons l'entier x_i construit et voyons comment l'on obtient x_{i+1}. On le cherche sous la forme $x_{i+1} = x_i + p^i r$ pour un certain entier r. Calculons :

$$\begin{aligned} P(x_{i+1}) &= a_0 + a_1 \left(x_i + p^i r\right) + a_2 \left(x_i + p^i r\right)^2 + \cdots + a_k \left(x_i + p^i r\right)^k \\ &\equiv a_0 + a_1 x_i + a_1 p^i r + a_2 x_i^2 + 2a_2 x_i p^i r + \cdots + a_k x_i^k + k a_k x_i^{k-1} p^i r \\ &\equiv P(x_i) + p^i r P'(x_i) \pmod{p^{i+1}} \end{aligned}$$

d'après la congruence rappelée au début de la preuve. D'après l'hypothèse de récurrence, il existe un entier q tel que $P(x_i) = qp^i$. Ainsi si l'on choisit r tel que $rP'(x_i) \equiv -q \pmod{p}$, on aura fini. Mais cela est possible car comme $x_i \equiv x_1 \pmod{p}$, on a $P'(x_i) \equiv P'(x_1) \pmod{p}$ qui est un résidu non nul et donc inversible. Ceci conclut l'existence.

L'unicité est laissée au lecteur : on peut pour la démontrer l'inclure dans l'hypothèse de récurrence et utiliser le fait que le r trouvé précédemment est uniquement déterminé modulo p. □

Remarque. Il existe des raffinements du lemme de Hensel qui peuvent être très utiles dans certains cas, mais qui requièrent un énoncé beaucoup plus lourd et difficilement mémorisable. En pratique, si le lemme de Hensel ne s'applique pas tel quel, il est souvent plus efficace de refaire la démonstration dans le cas particulier qui nous intéresse.

Les puissances modulo p^n

Malgré son apparence un peu complexe et technique, le lemme de Hensel admet de nombreuses applications. Par exemple, il peut être utile pour déterminer quels sont les *résidus quadratiques* (c'est-à-dire les carrés de résidus) modulo p^n. On a de fait la proposition suivante :

Proposition 3.6.2 *Soient p est un nombre premier impair et x un entier premier à p. Alors x est un résidu quadratique modulo p^n si, et seulement s'il en est un modulo p.*

Démonstration. Le sens direct est immédiat : si $x \equiv y^2 \pmod{p^n}$, alors on a également $x \equiv y^2 \pmod{p}$.

Pour la réciproque on utilise le lemme de Hensel. On pose $P(X) = X^2 - x$, et on a $P'(X) = 2X$. Par hypothèse il existe y tel que $x \equiv y^2 \pmod{p}$, *i.e.* $P(y) \equiv 0 \pmod{p}$. De plus on a forcément $y \not\equiv 0 \pmod{p}$, et donc $P'(y) = 2y \not\equiv 0 \pmod{p}$, puisqu'on a supposé p impair. Le lemme de Hensel fournit la conclusion attendue. □

Remarque. Évidemment cette proposition ne résout pas complètement le problème des résidus quadratiques puisqu'il reste à voir ce qui se passe modulo un nombre premier p. Ces résultats sont bien connus et détaillés dans le second tome de ce cours.

La proposition précédente se généralise directement à une situation plus vaste. On obtient :

Proposition 3.6.3 *Soient k un entier et p un nombre premier ne divisant pas k. Soit x un entier premier à p. Alors, pour tout entier n, le nombre x est une puissance k-ième modulo p^n si, et seulement s'il en est une modulo p.*

On peut alors se demander ce qu'il se passe lorsque k n'est plus premier à p. Dans ce cas, la situation est un peu plus complexe comme le montre le lemme suivant :

Lemme 3.6.4 *Si a et b sont des entiers tels $a \equiv b \pmod p$ alors $a^p \equiv b^p \pmod{p^2}$. Plus généralement, si pour un entier i, on a $a \equiv b \pmod{p^i}$, alors $a^{p^j} \equiv b^{p^j} \pmod{p^{i+j}}$ pour tout entier j.*

Démonstration. Pour le cas $j = 1$, on écrit $b = a + p^i q$ pour un certain entier q et on applique la congruence rappelée dans la démonstration du lemme de Hensel qui permet de conclure directement. Le cas général s'en déduit par récurrence immédiate. ☐

Si la proposition 3.6.3 s'étendait pour les k non premiers à p, tous les nombres premiers à p devraient être des puissances p-ième modulo p^2, puisqu'ils le sont tous modulo p (on rappelle que par le petit théorème de Fermat, on a $a^p \equiv a \pmod p$ pour tout entier a). Or le lemme précédent implique en particulier qu'il n'y a que p puissances p-ième modulo p^2.

Cependant, on dispose quand même d'un énoncé analogue à la proposition 3.6.3 pour le cas $k = p$:

Proposition 3.6.5 *Soit x un entier premier à p. Soit $n \geqslant 3$ un entier. Alors x est une puissance p-ième modulo p^n si, et seulement s'il en est une modulo p^3.*

Démonstration. Le sens direct est évident. Pour la réciproque, on ne peut pas utiliser le lemme de Hensel directement, mais on peut adapter la démonstration. Voyons sur cet exemple comment cela peut fonctionner.

On suppose qu'il existe x_3 tel que $x_3^p \equiv x \pmod{p^3}$. On construit à nouveau par récurrence une suite (x_n) d'entiers tels que $x_n \equiv x_3 \pmod p$ et $x_n^p \equiv x \pmod{p^n}$. Cependant, ici, on cherche x_{n+1} sous la forme $x_{n+1} = x_n + p^{n-1} r$. On obtient la relation :

$$x_{n+1}^p = \left(x_n + p^{n-1} r\right)^p \equiv x_n^p + p^n r \pmod{p^{n+1}}$$

puisque on a $n \geqslant 3$ (et donc $2(n-1) \geqslant n+1$). Par hypothèse de récurrence on a $x_n^p = a + p^n q$ pour un certain entier q. Il suffit pour conclure de choisir $r = -x_n' q$ où x_n' désigne un inverse de x_n modulo p (les entiers x_n' et p sont bien premiers entre eux, car on a supposé x premier avec p). ☐

3.7 Coefficients binomiaux

Définition 3.7.1 Soient n et k deux entiers. On pose :

$$\mathrm{C}_n^k = \begin{cases} \frac{n!}{k!(n-k)!} & \text{si } 0 \leqslant k \leqslant n \\ 0 & \text{sinon} \end{cases}$$

Propriétés immédiates

☞ Pour tout entier n, on a $\mathrm{C}_n^0 = \mathrm{C}_n^n = 1$

☞ Pour tous entiers n et k, on a $\mathrm{C}_n^k = \mathrm{C}_n^{n-k}$

☞ Pour tous entiers n et k, on a $k\mathrm{C}_n^k = n\mathrm{C}_{n-1}^{k-1}$

Les nombres C_n^k sont appelés *coefficients binomiaux*. Ils ont une interprétation combinatoire (C_n^k compte le nombre de parties à k éléments d'un ensemble de cardinal n) et ils apparaissent dans la formule du binôme de Newton que nous rappelons :

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^k b^{n-k}$$

Les remarques précédentes assurent que C_n^k est toujours un entier, ce que nous allons démontrer avec des arguments arithmétiques.

Proposition 3.7.2 *Soient n et k des entiers. Alors C_n^k est un entier.*

Démonstration. Soit p un nombre premier. On utilise la formule de Legendre pour évaluer la valuation p-adique de C_n^k. On a :

$$v_p(C_n^k) = v_p(n!) - v_p(k!) - v_p((n-k)!) = \sum_{i=1}^{\infty} \left(\left[\frac{n}{p^i}\right] - \left[\frac{k}{p^i}\right] - \left[\frac{n-k}{p^i}\right] \right)$$

On a vu que pour tous réels x et y, $[x+y] \geqslant [x] + [y]$, et donc chaque terme de la somme précédente est positif ou nul. Il en est donc de même de $v_p(C_n^k)$. Ceci étant valable pour tout nombre premier, on en déduit que C_n^k est entier. □

On peut parfois affiner la proposition précédente comme le montre l'exercice suivant (qui est un résultat important à retenir) :

<u>*Exercice*</u> : Soient $n = p^r$ une puissance d'un nombre premier p et k tel que $1 \leqslant k \leqslant p^r - 1$. Montrer que $C_{p^r}^k$ est un multiple de p.

<u>*Solution*</u> : On reprend :

$$v_p(C_{p^r}^k) = \sum_{i=1}^{\infty} \left(\left[\frac{p^r}{p^i}\right] - \left[\frac{k}{p^i}\right] - \left[\frac{p^r-k}{p^i}\right] \right)$$

Comme précedemment, chaque terme de la somme est positif ou nul. Mais cette fois-ci, lorsque $i = r$, on a :

$$\left[\frac{p^r}{p^r}\right] - \left[\frac{k}{p^r}\right] - \left[\frac{p^r-k}{p^r}\right] = 1 - 0 - 0 = 1$$

ce qui assure que la somme totale est supérieure ou égale à 1 et donc la conclusion.

√

Remarque. On aurait pu également utiliser $kC_{p^r}^k = p^r C_{p^r-1}^{k-1}$.

Triangle de Pascal

La formule suivante valable pour tous entiers n et k (qu'on laisse au lecteur le soin de vérifier) :

$$C_n^k = C_{n-1}^k + C_{n-1}^{k-1}$$

permet de calculer les coefficients binomiaux de proche en proche.

Pour des raisons pratiques, on rassemble souvent les C_n^k non nuls dans le *triangle de Pascal* :

$n \backslash k$	0	1	2	3	4	5
0	1					
1	1	1				
2	1	2	1			
3	1	3	3	1		
4	1	4	6	4	1	
5	1	5	10	10	5	1

La formule $\mathrm{C}_n^k = \mathrm{C}_{n-1}^k + \mathrm{C}_{n-1}^{k-1}$ implique qu'un nombre du tableau précédent est obtenu en additionnant les deux nombres placés au-dessus (celui juste au-dessus et son voisin de gauche).

La construction précédente s'avère très intéressante lorsque l'on souhaite déterminer les coefficients binomiaux modulo un nombre entier N. En effet, on remplit le tableau exactement de la même manière mais on ne tient compte que des restes modulo N lors des additions.

Lorsque $N = p$ est un nombre premier, on dispose en outre d'un théorème pour déterminer simplement C_n^k modulo p :

Théorème 3.7.3 (Lucas) *Soit p un nombre premier. Soient n et k des entiers avec $0 \leqslant k \leqslant n$. Écrivons les décompositions en base p de n et de k :*

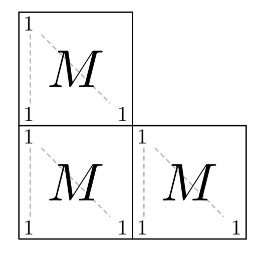
$$\begin{aligned} n &= n_d p^d + n_{d-1} p^{d-1} + \cdots + n_1 p + n_0 \\ k &= k_d p^d + k_{d-1} p^{d-1} + \cdots + k_1 p + k_0 \end{aligned}$$

où k_d peut valoir 0. Alors :

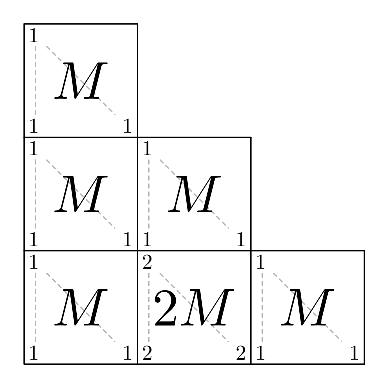
$$C_n^k \equiv C_{n_d}^{k_d} C_{n_{d-1}}^{k_{d-1}} \cdots C_{n_0}^{k_0} \pmod p$$

Démonstration. *Avec des dessins...*

Notons M le tableau carré $p \times p$ formé par les p premières lignes (donc pour n variant entre 0 et $p-1$) du triangle de Pascal modulo p. D'après l'exercice précédent, la première ligne qui n'est pas dans M ne contient que des 0 (modulo p) sauf pour les termes des colonnes 0 et p qui sont égaux à 1. Le procédé de construction du triangle de Pascal implique que les $2p$ premières lignes sont données par :



Mais alors, en continuant la construction, on voit que la ligne suivante ne contient que des 0 sauf à l'extrémité gauche (où il y a un 1), à la colonne p (où il y a un 2) et à la colonne $2p$ où il y a un 1. On obtient alors le dessin suivant :



Et ainsi de suite... et donc le terme C_n^k se retrouve être le nombre écrit à la position (n_0, k_0) dans le bloc situé à la position $\left(n_d p^{d-1} + \cdots + n_2 p + n_1, k_d p^{d-1} + \cdots + k_2 p + k_1\right)$, soit :

$$\mathrm{C}_n^k = \mathrm{C}_{n_d p^{d-1}+\cdots+n_2 p+n_1}^{k_d p^{d-1}+\cdots+k_2 p+k_1} \mathrm{C}_{n_0}^{k_0}$$

La conclusion découle alors d'une récurrence immédiate.

Avec des calculs...

On utilise ici la formule du binôme et l'égalité :

$$(1+X)^n = (1+X)^{n_0} (1+X)^{pn_1} \cdots (1+X)^{p^d n_d}$$

Le fait que p divise $\mathrm{C}_{p^r}^k$ pour $1 \leqslant k \leqslant p^r - 1$ prouve que $(1+X)^{p^r} \equiv 1 + X^{p^r} \pmod p$ pour tout entier r. Ainsi :

$$(1+X)^n = (1+X)^{n_0} (1+X^p)^{n_1} \cdots \left(1 + X^{p^d}\right)^{n_d}$$

On compare les termes en X^k. À gauche, le coefficient vaut C_n^k et à droite, comme k a une unique décomposition en base p qui est $k = k_d p^d + \cdots + k_1 p + k_0$, ce coefficient vaut :

$$\mathrm{C}_{n_d}^{k_d} \mathrm{C}_{n_{d-1}}^{k_{d-1}} \cdots \mathrm{C}_{n_0}^{k_0}$$

et la congruence est prouvée. □

<u>*Exercice*</u> : Soient p un nombre premier et r un entier strictement positif. Montrer que :

$$\mathrm{C}_{p^r}^p \equiv p^{r-1} \pmod{p^r}$$

<u>*Solution*</u> : On utilise la formule bien connue $p\mathrm{C}_{p^r}^p = p^r \mathrm{C}_{p^r-1}^{p-1}$ qui donne :

$$\mathrm{C}_{p^r}^p = p^{r-1} \mathrm{C}_{p^r-1}^{p-1}$$

En base p, $k = p-1$ a un seul chiffre, donc en reprenant les notations précédentes, $k_0 = p-1$ et $k_i = 0$ pour tout $i > 0$. D'autre part, $n = p^r - 1$ s'écrit avec r chiffres $p-1$, *i.e.* $n_0 = \ldots = n_{r-1} = p-1$ et $n_i = 0$ pour $i > r$. Finalement, d'après le théorème de Lucas :

$$\mathrm{C}_{p^r-1}^{p-1} \equiv \mathrm{C}_{p-1}^{p-1} (\mathrm{C}_{p-1}^0)^{r-1} \equiv 1 \pmod p$$

Cela termine l'exercice. √

3.8 Exercices

Exercice 111 Prouver que le produit de k entiers consécutifs est divisible par $k!$.

Exercice 112 Soit n un entier positif ou nul tel que pour tout $0 \leqslant k \leqslant n$, C_n^k est impair. Montrer que $n = 2^m - 1$ pour un entier m.

Exercice 113 Soient $n \geqslant 2$ progressions arithmétiques d'entiers, infinies dans les deux sens (c.à.d. indexées sur $\mathbb{Z}$), telles que deux quelconques d'entre elles aient toujours au moins un terme commun. Prouver qu'il existe un entier qui appartient à chacune des progressions arithmétiques.

Exercice 114 On note $\varphi(n)$ le nombre d'entiers compris entre 1 et n et premiers avec n. Prouver que :

$$\sum_{d|n} \varphi(d) = n$$

Exercice 115 La légende raconte que les chinois procédaient de la façon suivante pour compter leur armées. Le « général » demandait aux soldats de se mettre en rang deux par deux, et notait s'il restait un soldat isolé ou non. Il leur demandait ensuite de se mettre en rang trois par trois et notait encore le nombre de soldats isolés qu'il restait. On continuait ainsi, en se mettant en rang ensuite cinq par cinq, puis sept par sept, puis onze par onze, puis treize par treize et dix-sept par dix-sept.

Montrer que pour des armées de moins de cinq cent mille hommes, cette méthode permet effectivement de compter les soldats.

Exercice 116 (URSS 64) Soient a, b et n des entiers strictement positifs tels que, pour tout entier $k > 0$ avec $k \neq b$, le nombre $a - k^n$ soit divisible par $b - k$. Prouver que $a = b^n$.

Exercice 117 Montrer que pour tout entier n, $9^n - 2^n$ est divisible par 7.

Exercice 118 Déterminer tous les nombres premiers p tels que $4p + 1$ et $7p - 4$ soient également premiers.

Exercice 119* (TDV 04) Existe-t-il une permutation $\{a_1, \ldots, a_{2004}\}$ de $\{1, \ldots, 2004\}$ de sorte que $a_i + \cdots + a_{i+9}$ soit un multiple de 10 pour tout i compris entre 1 et 1995 ?

Exercice 120* (AMM, France 03) On se place dans le plan rapporté à un repère orthonormal (O, i, j). On dit qu'un point à coordonnées entières A est invisible si le segment $[OA]$ contient un point à coordonnées entières distinct de O et de A. Soit L un entier naturel. Montrer qu'il existe un carré dont les côtés sont parallèles aux axes et ont une longueur égale à L et tel que tous les points à coordonnées entières intérieurs au carré soient invisibles.

Exercice 121* Calculer la somme des diviseurs de 104060401.

Exercice 122* Montrer que pour tout nombre premier $p \geqslant 3$, le numérateur de la fraction :

$$1 + \frac{1}{2} + \ldots + \frac{1}{p-1}$$

est divisible par p.

Exercice 123* Existe-t-il deux puissances de 2 distinctes ayant exactement les mêmes chiffres (comptés avec multiplicité) en base 10. (Les éventuels zéros au début d'un nombre ne sont pas comptés comme des chiffres).

Exercice 124* (Putnam 50) Soit n un entier. Prouver que le nombre de k tel que C_n^k est impair est une puissance de 2.

Exercice 125* Prouver qu'il n'existe pas de suite infinie (x_n) de nombres premiers telle que, pour tout n, on ait $|x_{n+1} - 2x_n| = 1$.

Exercice 126* (Russie 95) Existe-t-il une permutation $\{a_1, a_2, a_3, \ldots\}$ de $\mathbf{N}^\star$ telle que, pour tout n, le nombre $a_1 + a_2 + \cdots + a_n$ soit divisible par n ?

Exercice 127* Soient 111 entiers relatifs de somme nulle. Montrer que la somme de leur puissances 37-ièmes est divisible par 399.

Exercice 128* (OIM 79) Soient a et b des entiers strictement positifs vérifiant :

$$\frac{a}{b} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \ldots - \frac{1}{1318} + \frac{1}{1319}$$

Montrer que 1979 divise a.

Exercice 129* (Crux Mathematicorum) Trouver tous les nombres premiers p pour lesquels il existe une base $b \geqslant 2$ dans laquelle l'écriture de p utilise une et une seule fois tous les chiffres. (Le chiffre 0 peut se positionner au début de l'écriture).

Exercice 130* (OIM 86) Soit d un entier strictement positif n'appartenant pas à l'ensemble $\{2, 5, 13\}$. Montrer que l'on peut trouver un couple (a, b) d'éléments distincts de l'ensemble $\{2, 5, 13, d\}$ tel que $ab - 1$ ne soit pas le carré d'un entier.

Exercice 131* (Estonie 00, France 04) Existe-t-il un entier n pour lequel on puisse partitionner l'ensemble $\{n, \ldots, n + 17\}$ en deux parties A et B telles que le produit des éléments de A vaut celui des éléments de B ?

Exercice 132* Pour x et y dans $\mathbf{N}$, on pose :

$$\begin{aligned} B &= x\,(y+1) - (y! + 1) \\ f\,(x,y) &= \frac{y-1}{2}\left(\left|B^2 - 1\right| - \left(B^2 - 1\right)\right) + 2 \end{aligned}$$

Montrer que, lorsque x et y décrivent $\mathbf{N}$, la fonction f décrit exactement l'ensemble des nombres premiers, et que chaque nombre premier impair est atteint une seule fois.

Exercice 133* Soient p un nombre premier différent de 2 et 5 et n un entier strictement positif. Montrer que la somme :

$$\frac{1}{n} + \frac{1}{n+1} + \cdots + \frac{1}{n+p-1}$$

n'est jamais un nombre décimal (*i.e.* sa partie décimale est finie). Que se passe-t-il pour $p = 2$ et $p = 5$?

Exercice 134* (Bosnie 97) a) Prouver que, pour tout entier $n > 0$, il existe un ensemble M_n contenant exactement n entiers strictement positifs et tel que : les moyennes arithmétiques et géométriques des éléments de toute partie non vide de M_n sont des entiers.

b) Existe-t-il un ensemble infini d'entiers naturels ayant la même propriété ?

Exercice 135* (Roumanie 94) On construit une suite d'entiers en posant $u_0 = 2000^{2003}$ et pour tout $n \geqslant 0$, $u_{n+1} = u_n + 7$ si u_n est impair, $u_{n+1} = \frac{u_n}{2}$ si u_n est pair.

Quel est le plus petit entier atteint par cette suite u_n ?

Exercice 136* (SL 84) Montrer que pour tout $n > 0$, C_{2n}^{n} divise $\text{PPCM}\,(1, \ldots, 2n)$.

Exercice 137* Soit p un nombre premier. Prouver qu'il existe un diviseur premier de $p^p - 1$ qui est congru à 1 modulo p.

Exercice 138* Soient $n_1, \ldots, n_k$ des entiers positifs. Montrer que le quotient :

$$\frac{(n_1 + \ldots + n_k)!}{n_1! \ldots n_k!}$$

est entier.

Exercice 139* (Nombres de Catalan) Montrer que pour tout n, C_{2n}^{n} est divisible par $n + 1$.

Exercice 140* Trouver tous les entiers strictement positifs n tels que 17 divise $3^n - n$.

Exercice 141* (OIM 72) Montrer que $(2m)!\,(2n)!$ est un multiple de $m!n!\,(m + n)!$ pour tous entiers positifs ou nuls m et n.

Exercice 142* (SL 85) Soient $k \geqslant 2$ et $n_1, \ldots, n_k$ des entiers strictement positifs tels que :

$$\begin{array}{rcl} n_2 & \text{divise} & 2^{n_1} - 1 \\ n_3 & \text{divise} & 2^{n_2} - 1 \\ & \vdots & \\ n_{k-2} & \text{divise} & 2^{n_{k-1}} - 1 \\ n_1 & \text{divise} & 2^{n_k} - 1 \end{array}$$

Prouver que $n_1 = n_2 = \cdots = n_k = 1$.

Exercice 143* (Iran 94) Soit $p \geqslant 5$ un nombre premier. Montrer que 43 divise $7^p - 6^p - 1$.

Exercice 144* Déterminer tous ls entiers $a > 0$ et $b > 2$ tels que $2^a + 1$ soit divisible par $2^b - 1$.

Exercice 145 (Balkan 89 (non utilisé))** Montrer que pour tout $n \geqslant 3$, le nombre :

$$n^{n^{n^n}} - n^{n^n}$$

est divisible par 1989.

Exercice 146 (France 04)** On note $\mathcal{P}$ l'ensemble des nombres premiers. On considère une partie M de $\mathcal{P}$ ayant au moins 3 éléments. On suppose que, pour tout sous-ensemble fini non vide strict A de M, les facteurs premiers de l'entier :

$$\left(\prod_{p \in A} p\right) - 1$$

appartiennent à M. Montrer que $M = \mathcal{P}$.

Exercice 147 (SL 91)** Déterminer le PGCD des nombres $n^{37} - n$ pour n décrivant $\mathbf{Z}$.

Exercice 148 (SL 91)** Prouver que le dernier chiffre non nul de $n!$ forme une suite non périodique (même à partir d'un certain rang).

Exercice 149 (Moscou 73)** Douze peintres vivent dans douze maisons d'une même rue circulaire, peintes certaines en bleu et les autres en blanc. Chaque fin de mois, l'un des peintres quitte sa maison avec ses pots de peinture et repeint chaque maison de la couleur contraire, en commençant par la sienne et dans l'ordre des aiguilles d'une montre. Il s'arrête dès qu'il a repeint une maison blanche en bleu. Durant une année, un peintre donné ne fait cela qu'une seule fois. Prouver que, si au début de l'année l'une au moins des maisons était peinte en bleu alors, à la fin de l'année, chacune retrouvera sa couleur initiale.

Exercice 150 (Quadrature)** Trouver toutes les puissances de 2 qui sont encore des puissances de 2 lorsqu'on efface leur chiffre de gauche.

Exercice 151 (Russie 96)** Prouver qu'il n'existe pas d'entiers a et b strictement positifs tels que, pour tous nombres premiers distincts p et q strictement supérieurs à 1000, le nombre $ap + bq$ soit aussi premier.

Exercice 152 (Turquie 96)** Soient a et n des entiers strictement positifs. Prouver que :

$$\prod_{k=0}^{n-1} (a^n - a^k)$$

est divisible par $n!$.

Exercice 153 (OIM 75)** Soient A la somme des chiffres (en base 10) de 4444^{4444}, et B la somme des chiffres de A. Calculer la somme des chiffres de B.

Exercice 154 (D. J. Newman)** Soient a et b des entiers strictement positifs. Montrer que le nombre :

$$\left(a + \frac{1}{2}\right)^n + \left(b + \frac{1}{2}\right)^n$$

est un entier pour seulement un nombre fini de valeurs de n.

Exercice 155** Soit $n > 1$ un entier. Prouver qu'il existe un entier $k > 0$ tel que $2k + 1$ divise $n + k!$ ou $n - k!$. (On pourra utiliser, après l'avoir prouvé, qu'un diviseur premier impair de $n^2 + 1$ est toujours congru à 1 modulo 4).

Exercice 156** Soient n et m deux entiers. Montrer que :

$$\frac{(nm)!}{m!\,(n!)^m}$$

est un entier.

Exercice 157* (Erdös et al.)** Soit $n \geqslant 1$ un entier. Prouver que parmi $2n - 1$ entiers, on peut toujours en trouver n dont la somme est divisible par n.

Exercice 158*** n enfants sont assis en cercle. Dolpha donne un bonbon au premier enfant, saute le second, donne un bonbon au troisième, saute les deux suivants, donne un bonbon au prochain enfant, puis saute les trois suivants, et ainsi de suite. Pour quelle valeur de n, tous les enfants auront-ils au moins un bonbon au bout d'un certain nombre de tours ?

Exercice 159* (Erdös)** Prouver que le produit des nombres premiers inférieurs ou égaux à n est inférieur ou égal à 4^n.

Exercice 160* (USA 82)** Montrer qu'il existe un entier k tel que $k2^n + 1$ est toujours composé pour tout n.

Exercice 161* (SL 98)** Déterminer tous les entiers $n > 0$ pour lesquels il existe un entier m tel que $2^n - 1$ divise $m^2 + 9$.

Exercice 162* (France 02)** Soit p un nombre premier impair. Montrer qu'il existe p entiers strictement positifs $a_1, a_2, \cdots, a_p$ inférieurs ou égaux à $2p^2$ tels que les $\frac{p(p-1)}{2}$ sommes de la forme $a_i + a_j$ (où $i < j$) soient distinctes.

Exercice 163*** Trouver tous les entiers $n \geqslant 1$ tels que n divise $2^{n-1} + 1$.

Exercice 164* (SL 93)** Soit $b > 1$ un entier. Soit a un entier strictement positif tel que $b^n - 1$ divise a. Montrer qu'en base b, l'entier a possède au moins n chiffres non nuls.

Exercice 165** (SL 97)** Montrer que toute progression arithmétique infinie d'entiers positifs qui contient un carré et un cube contient une puissance sixième.

Exercice 166**** Pour tout entier $n \geqslant 1$, on écrit :

$$1 + \frac{1}{2} + \ldots + \frac{1}{n} = \frac{a(n)}{b(n)}$$

avec $a(n)$ et $b(n)$ premiers entre eux. Montrer qu'il existe une infinité d'entiers n pour lesquels $a(n)$ n'est pas une puissance d'un nombre premier.

4 Équations diophantiennes

On appelle *équation diophantienne*[5] toute équation dont on cherche les solutions en nombres entiers. Par exemple $x^2 = 4k + 3$, $x^2 + y^2 = z^2$, $1! + 2! + \cdots + n! = x^2$ sont des équations diophantiennes.

Notez qu'en général, les équations diophantiennes font intervenir plusieurs et souvent un grand nombre d'inconnues. Notez également que les techniques utilisées pour aborder les équations sont très souvent radicalement différentes des techniques classiques d'attaque pour les équations algébriques.

Résoudre celles-ci est souvent très difficile et les mathématiques actuelles sont encore loin de savoir proposer des méthodes dans tous les cas. Toutefois, certaines pistes sont très bien balisées et ce sont elles que nous allons présenter par la suite.

Finalement, ne soyez pas effrayés : s'il est fort probable que si vous inventiez une équation diophantienne un peu tordue, elle soit complètement inabordable même pour les plus grands chercheurs, il est aussi évident que les exercices que l'on vous propose disposent de solutions que vous avez les moyens de trouver.

4.1 Quelques réflexes

Les propriétés des entiers et les notions de divisibilité sont essentielles dans la résolution des équations diophantiennes. Rappelons tout de suite quelques propriétés qu'il est bon d'avoir constamment en tête :

Quelques idées à tester systématiquement

☞ Si le produit ab est une puissance d'un nombre premier p, alors a et b sont également des puissances de ce nombre premier. Si le produit ab est une puissance d'un entier n, il peut être intéressant de décomposer n en facteurs premiers.

☞ Si le produit ab est un carré et que a et b sont premiers entre eux, alors a et b sont des carrés. Plus généralement si $d = \text{PGCD}\,(a, b)$, a s'écrit dx^2 et b s'écrit dy^2 pour des entiers x et y. Rappelons à ce niveau que le PGCD de deux entiers dont la différence est n est un diviseur de n. En particulier, cette propriété est forte utile pour les situations faisant intervenir des produits $a\,(a + n)$ ou plus souvent $(a - n)\,(a + n) = a^2 - n^2$.

☞ Un entier strictement positif est supérieur ou égal à 1. De même, si n est entier et $n \leqslant x$, alors $n \leqslant [x]$. Un bon reflexe à avoir à ce niveau est de ne jamais (ou du moins le plus rarement possible) conserver des inégalités strictes entre nombres entiers : elles peuvent toujours être améliorées.

☞ On dispose de la factorisation :

$$a^n - b^n = (a - b)\left(a^{n-1} + a^{n-2}b + \cdots + b^{n-1}\right)$$

et si n est impair, de la factorisation analogue :

$$a^n + b^n = (a + b)\left(a^{n-1} - a^{n-2}b + \cdots + b^{n-1}\right)$$

[5] Du nom du mathématicien Diophante.

Ces factorisations s'avèrent très utiles lorsque l'on a besoin de modifier l'aspect d'une équation diophantienne, le plus souvent en faisant des manipulations algébriques. Signalons également que toute expression de la forme $\alpha x + \beta y + \gamma xy + \delta$ peut en général se factoriser sous la forme :

$$(ax + b)(cx + d) + e$$

pour certains rationnels (pas forcément entiers même si α, β, γ et δ le sont) a, b, c, d et e.

Voyons sur des exemples simples comment utiliser ces idées. Cherchons dans un premier temps à résoudre :

$$2^n + 1 = x^2$$

Pour cela, on fait passer le 1 de l'autre côté de l'égalité et on factorise :

$$2^n = (x + 1)(x - 1)$$

et donc d'après une des propriétés rappelées précédemment, à la fois $x + 1$ et $x - 1$ doivent être des puissances de 2. Or, des puissances de 2 qui diffèrent de 2, il n'y a que 2 et 4. Donc $x = 3$ est la seule solution, et fournit $n = 3$.

Cet exemple illustre de façon parfaite le fait mentionné précédemment stipulant qu'il peut parfois être intéressant de faire des manipulations algébriques simples sur l'équation pour lui donner un aspect plus propice à sa résolution. Souvent savoir factoriser un membre de l'égalité s'avère déterminant.

Lorsque seulement deux valeurs interviennent, un premier pas éclairant consiste souvent à comparer les ordres de grandeur de ces valeurs. Pour exemple, considérons l'équation :

$$x^2 = 2 + 6y^2 + y^4$$

Sans trop réfléchir, on voit que si cette équation admet une solution, x doit être de l'ordre de y^2 et même plus précisément l'écriture suivante :

$$x^2 = (y^2 + 3)^2 - 7$$

nous dit que x ne doit pas être loin de $y^2 + 3$. Précisément en fait, on a $x < y^2 + 3$. On a également :

$$x^2 = (y^2 + 2)^2 + 2y^2 - 2$$

et donc dès que $2y^2 - 2 > 0$, on doit avoir $x > y^2 + 2$. Comme il n'y a pas d'entiers entre $y^2 + 2$ et $y^2 + 3$ l'équation n'admet pas de solution. Les seules solutions éventuelles seraient alors obtenues pour les y tels que $2y^2 - 1 \geqslant 0$, c'est-à-dire $y = -1$, $y = 0$ et $y = 1$. On vérifie ensuite au cas pas cas.

La morale est que lorsque l'équation a un petit nombre d'inconnues, des techniques d'inégalité, peuvent permettre de restreindre l'étude à un nombre fini de cas. Lorsque l'exercice est bien fait, ce nombre est petit, et on peut donc traiter ces cas un par un.

Une autre illustration simple de ce dernier principe est le suivant : trouver tous les entiers positifs n tel que $3n+7$ divise $5n+13$. Le quotient $\frac{5n+13}{3n+7}$ est toujours compris strictement entre 0 et 2 et donc, comme il est entier, il ne peut en fait valoir que 1. Il ne reste alors plus qu'à résoudre l'équation $5n+13 = 3n+7$ qui admet pour solution $n = -3$. Ce nombre n'est pas positif, donc il n'existe aucun n répondant à notre question.

Remarquons pour finir que l'utilisation d'inégalités peut s'avérer efficace même si le nombre d'inconnues est plus important. Pour exemple, nous donnons l'exercice suivant :

Exercice : Trouver tous les entiers strictement positifs x, y et z tels que :

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 1$$

Solution : Comme les inconnues jouent un rôle symétrique, on peut supposer $0 < x \leqslant y \leqslant z$. Dans ces conditions, on a :

$$1 = \frac{1}{x} + \frac{1}{y} + \frac{1}{z} \leqslant \frac{3}{x}$$

et donc $x \leqslant 3$. Il ne peut valoir 1, il vaut donc 2 ou 3.

On traite les deux cas séparemment en utilisant à nouveau la même méthode. Si $x = 2$, l'équation devient :

$$\frac{1}{y} + \frac{1}{z} = \frac{1}{2}$$

puis par le même argument $x = 2 \leqslant y \leqslant 4$. On teste alors les cas un par un trouve que les seules solutions sont $y = 3$, $z = 6$ et $y = 4$, $z = 4$.

Pour $x = 3$, on obtient :

$$\frac{1}{y} + \frac{1}{z} = \frac{2}{3}$$

puis $x = 3 \leqslant y \leqslant 3$. La seule solution est, dans ce cas, $x = y = 3$.

Finalement, les solutions sont les triplets $(2,3,6)$, $(2,4,4)$, $(3,3,3)$ et toutes leurs permutations. $\surd$

Confrontés à une équation, on peut également se demander s'il n'y a pas une manipulation simple qui permet de transformer une solution en une autre. Par exemple, il est possible qu'en multipliant tous les entiers d'une solution par une même valeur d, on obtienne une nouvelle solution. On dit souvent alors que l'équation est *homogène*. Ce cas se produit par exemple lorsque l'équation proposée est une somme de mônomes, tous de même degré. Souvent la solution obtenue ainsi est « plus grande ». Cependant cela peut-être encore plus intéressant si elle se trouve « plus petite » (voir 4.3).

Ces manipulations permettent par exemple de faire des hypothèses supplémentaires sur une solution recherchée. Par exemple, dans le cas « homogène » présenté précédemment, on peut supposer que les inconnues sont premières entre elles dans leur ensemble. Ces solutions sont souvent appelées *fondamentales*. Les autres solutions (différentes de $(0,0,\dots,0)$ qui convient toujours dans ce cas) s'obtiennent alors par multiplication à partir d'une solution fondamentale. Ainsi, si on trouve toutes les solutions fondamentales, on aura trouvé toutes les solutions.

Cette dernière remarque est par exemple appliquée dans la preuve usuelle de l'irrationnalité de $\sqrt{2}$. On se ramène directement à montrer que l'équation diophantienne :

$$a^2 = 2b^2$$

n'a pas de solution non nulle. On remarque que l'équation est homogène et il suffit donc de chercher les solutions avec PGCD $(a, b) = 1$. On remarque ensuite que a^2 est pair, donc a doit être pair. Ceci implique que a^2 est un multiple de 4, et donc b^2 est pair. Ainsi b est pair, et il n'y a pas de solution avec a et b premiers entre eux.

La remarque sur l'homogénéïté implique alors qu'il n'y a aucune solution hormis la solution triviale $a = b = 0$. Cela démontre l'irrationnalité de $\sqrt{2}$.

Noter que parfois, la manière dont on transforme une solution en une autre est moins évidente. Par exemple, pour l'équation suivante :

$$x^3 + y^5 = z^2$$

il faut remarquer que si (x, y, z) est solution et si a est un entier quelconque, alors le triplet $(a^{10}x, a^6y, a^{15}z)$ est aussi solution. Si l'on demande ensuite simplement de prouver que cette équation admet une infinité de solutions en entiers strictement positifs, on conclut en remarquant que $(2, 1, 3)$ est solution.

On a ainsi prouvé que pour tout entier a, le triplet $(2a^{10}, a^6, 3a^{15})$ est solution, ce qui en fait bien une infinité.

De façon plus générale, lorsque l'on souhaite prouver que telle équation admet une infinité de solutions, il s'agit souvent de trouver une formule. L'exemple de l'équation :

$$x^3 + y^3 + z^3 + t^3 = 3$$

est frappant. Pour conclure, il suffit de sortir de son chapeau l'identité :

$$\left(4 + 24n^3\right)^3 + \left(4 - 24n^3\right)^3 + \left(-24n^2\right)^3 + (-5)^3 = 3$$

On pourrait objecter qu'on ne voit pas trop comment on peut arriver à une telle formule. En réalité, si l'on sait ce que l'on cherche, à force de patience et avec un peu de pratique, on arrive assez bien à bricoler des coefficients qui conviennent.

4.2 Utilisation des congruences

Une méthode, souvent efficace, pour prouver qu'une équation diophantienne n'a *pas* de solution est de considérer la même équation modulo un entier N et de prouver qu'il n'y a pas de solution dans cette nouvelle situation.

Le premier exemple à considérer est celui de l'équation :

$$x^2 = 4k + 3$$

S'il existait un couple (x, k) solution, alors il vérifierait la congruence :

$$x^2 \equiv 4k + 3 \equiv 3 \pmod 4$$

mais on a vu que les seuls carrés modulo 4 sont 0 et 1. On en déduit que l'équation de départ n'a pas de solution.

Il n'y a pas beaucoup de théorie à faire sur le sujet, le point délicat est de trouver un entier N qui amènera une contradiction lorsque l'on regarde modulo N. Pour cela, on a quelques principes généraux :

- ☞ Lorsque l'équation fait intervenir des carrés, il est souvent intéressant de regarder modulo 4, voire 8 ou 16 (et il est peu utile d'aller au delà – voir proposition 3.6.3). Retenez que les carrés modulo 4 sont toujours congrus à 0 ou 1, qu'ils sont toujours congrus à 0, 1 ou 4 modulo 8 et qu'ils sont toujours congrus à 0, 1, 4 et 9 modulo 16. (Il est utile de connaître ces résultats par cœur bien que ce soit facile de les retrouver en dressant une table).
- ☞ De façon plus générale, si p est un nombre premier et que l'équation fait intervenir des puissances de p, il peut être bon de regarder modulo p^2 ou p^3, voire les suivants...
- ☞ Lorsque l'on fait la liste des carrés modulo un nombre premier p, l'égalité $x^2 = (-x)^2$ entraîne que l'on ne pourra pas obtenir tous les restes possibles. En réalité, on en obtient exactement $\frac{p-1}{2}$. Lorsque l'on a des puissances n-ièmes qui apparaissent (disons avec n impair), cet argument ne fonctionne plus. Par contre, il reste vrai que de nombreux restes ne sont pas des puissances n-ième lorsque le modulo p est un nombre *premier* congru à 1 modulo n. Cette remarque est on ne peut plus intéressante lorsque l'équation fait intervenir deux types de puissances : par exemple, si on a un terme en x^2 et un en y^3, on pourrait être tenté de regarder modulo 7.
- ☞ Si l'équation fait intervenir un terme de la forme 2^n, on pourra également regarder modulo 2, 4, 8, etc. Ainsi, le terme en question va s'annuler à partir d'une certaine valeur de n. De même si on a un terme de la forme 3^n, on aura intérêt modulo 3, 9, et ainsi de suite.
- ☞ De façon un peu plus générale, si une constante, semble-t-il un peu étrange, intervient comme un facteur multiplicatif, il peut être opportun de regarder modulo cette constante. En effet, on tuera ainsi le terme correspondant.
- ☞ Encore si l'on a un terme de la forme a^n (où a est fixé et n est l'inconnue), on peut chercher un modulo N (pas démesurément trop grand) diviseur de $a^k - 1$ pour un certain entier k (pas trop grand, par exemple $k = 1$). En effet, dans ce cas, on aura $a^k \equiv 1 \pmod N$ et donc la suite des a^n modulo N sera périodique de période (divisant) k. Ainsi si k n'est pas choisi trop grand, le terme a^n ne pourra prendre qu'un petit nombre de valeurs modulo N. Par exemple, dans le cas des puissances de 2, on pourra choisir $N = 3$, $N = 5$ ou $N = 31$.

Les heuristiques données précédemment ne doivent pas etre considérées comme parole d'évangile. Parfois, il peut être préférable de suivre son intuition.

<u>*Exercice*</u> : Trouver tous les entiers relatifs x et y tels que :

$$x^2 = y^5 - 4$$

Solution : Comme les exposants qui interviennent dans l'équation sont 2 et 5, il peut être intéressant de l'examiner en réduction modulo un nombre premier p tel que 2 et 5 divisent $p-1$. Le premier qui se présente est $p = 11$.

Les puissances cinquièmes modulo 11 sont 0, 1 et -1, donc le second membre de l'équation est congru à 7, 8 ou 6 modulo 11. Par ailleurs, les carrés modulo 11 sont 0, 1, 4, 9, 5 et 3. Il en résulte immédiatement que l'équation n'a pas de solution. $\surd$

Remarquons pour finir qu'il existe des équations diophantiennes n'admettant pas de solutions, mais qui en admettent modulo N pour tout entier N. L'exemple de base est donné par l'exercice suivant :

Exercice : Montrer que l'équation :

$$\left(x^2-2\right)\left(x^2+7\right)\left(x^2+14\right)=0$$

n'admet pas de solution entière mais admet une solution modulo N pour tout entier non nul N. On pourra utiliser le critère d'Euler (qui sera discuté dans le second tome) qui affirme que si p est un nombre premier impair et a un entier premier à p, alors a est un carré modulo p si, et seulement si :

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p$$

Solution : Déjà, il est facile de voir que les seules solutions réelles de l'équation sont $\sqrt{2}$ et $-\sqrt{2}$ qui ne sont pas des entiers.

Considérons p un nombre premier impair et montrons que soit 2, soit -7, soit -14 est un carré modulo p. Remarquons que pour tout a premier à p, le carré de $a^{\frac{p-1}{2}}$ est congru à 1 modulo p et donc on a la factorisation :

$$\left(a^{\frac{p-1}{2}}-1\right)\left(a^{\frac{p-1}{2}}+1\right) \equiv 0 \pmod p \qquad (1)$$

Ainsi p divise un des deux facteurs. Supposons que ni 2, ni -7 ne soit un carré modulo p. Alors d'après le critère d'Euler, p ne divise pas le premier facteur de (1) lorsque $a = 2$ ou $a = -7$. C'est donc qu'il divise le second facteur et que l'on a les congruences :

$$\begin{aligned} 2^{\frac{p-1}{2}} &\equiv -1 \pmod p \\ (-7)^{\frac{p-1}{2}} &\equiv -1 \pmod p \end{aligned}$$

et en multipliant ces deux congruences, on arrive à :

$$(-14)^{\frac{p-1}{2}} \equiv 1 \pmod p$$

ce qui prouve que -14 est un carré modulo p.

On vient donc de prouver que 2, -7 ou -14 est un carré modulo p, et donc l'équation :

$$\left(x^2-2\right)\left(x^2+7\right)\left(x^2+14\right) \equiv 0 \pmod p$$

a bien une solution. D'après la proposition 3.6.3, cette équation a également une solution modulo p^n pour tout entier n (on utilise ici encore une fois le fait que p est impair).

Soit $N = 2^k$ une puissance de 2. Montrons que -7 est un carré modulo N. Pour $k \leqslant 3$, on vérifie que l'on a $3^2 \equiv -7 \pmod{2^k}$. On applique ensuite le proposition 3.6.5 qui conclut directement.

En résumé, on a prouvé que notre équation admet une solution modulo p^k pour tout nombre premier p et tout exposant k. Notons $P(X) = (X^2 - 2)(X^2 + 7)(X^2 + 14)$. Soit N un entier et $N = p_1^{\alpha_1} \cdots p_d^{\alpha_d}$ sa décomposition en facteurs premiers. On sait qu'il existe des entiers x_i tels que :

$$\begin{aligned} P(x_1) &\equiv 0 \pmod{p_1^{\alpha_1}} \\ P(x_2) &\equiv 0 \pmod{p_2^{\alpha_2}} \\ &\vdots \\ P(x_d) &\equiv 0 \pmod{p_d^{\alpha_d}} \end{aligned}$$

Soit x un entier tel que $x \equiv x_i \pmod{p_1^{\alpha_1}}$ pour tout entier i (qui existe d'après le lemme chinois). Il vérifie bien $P(x) \equiv 0 \pmod{N}$. $\surd$

Lorsqu'il existe un entier N pour lequel une équation diophantienne donnée n'admet pas de solution modulo N, on dit qu'il y a *obstruction locale*. Nous venons donc de voir qu'il peut y avoir des obstructions d'autre nature pour empêcher l'existence de solutions entières. L'étude de ces obstructions a occupé et occupe encore beaucoup de mathématiciens en géométrie algébrique.

4.3 Descente infinie

La *descente infinie* est une méthode introduite et abondamment utilisée par Fermat. Le but est de prouver qu'une certaine équation diophantienne n'admet pas (ou très peu) de solutions. Pour cela, on part d'une solution hypothétique et on en construit une nouvelle, strictement plus petite dans un certain sens.

On obtiendrait ainsi une suite strictement décroissante de solutions, ce qui n'est en général pas possible (de la même façon qu'il n'existe aucune suite infinie d'entiers positifs strictement décroissante).

Un premier exemple simple qui illustre ce principe est à nouveau l'irrationalité de $\sqrt{2}$. On est à nouveau amené à considérer l'équation :

$$a^2 = 2b^2$$

On prouve que a est pair puis que b l'est, et on voit que $\left(\frac{a}{2}, \frac{b}{2}\right)$ est une nouvelle solution. D'autre part si $b \neq 0$, on a $\left|\frac{b}{2}\right| < |b|$ (voici notre condition de décroissance).

Ainsi, si l'on part d'une solution (a_0, b_0) avec $b_0 \neq 0$, on peut construire une nouvelle solution (a_1, b_1) (en l'occurrence $a_1 = \frac{a}{2}$ et $b_1 = \frac{b}{2}$) avec $|b_1| < |b_0|$. Puis on continue, on construit (a_2, b_2), (a_3, b_3), et ainsi de suite. On construit ainsi une suite (b_i) telle que :

$$|b_0| > |b_1| > |b_2| > \cdots$$

ce qui constitue une contradiction.

Ainsi on a forcément $b = 0$ puis directement $a = 0$, et $\sqrt{2}$ est à nouveau irrationnel.

Voici, en exercice, un autre exemple tout à fait similaire :

Exercice : Trouver tous les entiers x, y et z tels que :

$$x^3 + 9y^3 = 3z^3$$

Solution : On part d'une éventuelle solution (x, y, z) distincte du triplet $(0, 0, 0)$. L'équation implique que x^3 est multiple de 3, et donc x l'est aussi. Mais alors $x = 3x'$ et l'équation devient (après simplification par 3) :

$$9x'^3 + 3y^3 = z^3$$

et on déduit de cela que z est multiple de 3. On écrit $z = 3z'$, l'équation devient :

$$3x'^3 + y^3 = 9z'^3$$

et on obtient 3 divise y. Posons $y' = \frac{y}{3}$. On vérifie que le triplet (x', y', z') est encore solution de l'équation de départ et qu'il est plus petit dans le sens :

$$|x'| + |y'| + |z'| < |x| + |y| + |z|$$

Le principe de descente infinie permet alors de conclure que l'unique solution est $x = y = z = 0$. $\checkmark$

Notons que ces deux cas relèvent encore de ce que l'on appelle une obstruction locale. Ici, il y a une solution, donc évidemment, il y a une solution modulo N pour tout entier N. Cependant, pour l'irrationalité de $\sqrt{2}$ par exemple, on a exactement (!) prouvé que si $a^2 \equiv 2b^2 \pmod{2^k}$, alors $a \equiv b \equiv 0 \pmod{2^k}$. Ainsi une éventuelle solution devrait être telle que $a \equiv b \equiv 0 \pmod{2^k}$ pour tout entier k et les seuls entiers vérifiant cela sont $a = b = 0$.

L'argument est exactement le même pour le second exemple, sauf que 2 est remplacé par 3.

Obstruction globale

Le principe de descente infinie s'applique toutefois dans des situations différentes. L'exemple le plus classique est celui du cas particulier de l'équation de Fermat pour $n = 4$. Pour l'illustrer nous allons avoir besoin du théorème suivant :

Théorème 4.3.1 (Triplets pythagoriciens) *Soient x, y et z des entiers positifs premiers entre eux dans leur ensemble vérifiant :*

$$x^2 + y^2 = z^2$$

Alors, soit x, soit y est pair. Dans le cas où c'est x qui l'est, il existe des entiers m et n premiers entre eux et de parité contraire tels que $x = 2mn$, $y = m^2 - n^2$ et $z = m^2 + n^2$.

Remarque. On vérifie immédiatement que réciproquement, les triplets fournis par le théorème précédent sont effectivement solutions de l'équation $x^2 + y^2 = z^2$. On a ainsi entièrement résolu cette équation.

Démonstration. Si d est un diviseur commun de x et y, alors d^2 divise $x^2 + y^2$ et donc z^2. Ainsi d divise z et d est un diviseur commun de x, y et z et d'après l'hypothèse $d = 1$. Finalement, x et y sont premiers entre eux. De même on prouve que x, y et z sont premiers entre eux deux à deux.

Si x et y étaient tous les deux impairs, on aurait $x^2 \equiv y^2 \equiv 1 \pmod 4$, et donc $z^2 = x^2 + y^2 \equiv 2 \pmod 4$, ce qui est impossible. Au moins l'un des deux est pair. Supposons que ce soit x et écrivons $x = 2x'$.

L'équation devient alors :

$$4x'^2 = (z - y)\,(z + y)$$

Les deux facteurs $z - y$ et $z + y$ sont de même parité et donc tous les deux pairs. En outre, si d est un diviseur commun de $z - y$ et de $z + y$, il divise leur somme et leur différence, c'est-à-dire $2z$ et $2y$ et donc 2 puisque y et z sont premiers entre eux. Cela prouve que les entiers $\frac{z-y}{2}$ et $\frac{z+y}{2}$ sont premiers entre eux. Leur produit est un carré, ce sont donc tous les deux des carrés :

$$\frac{z - y}{2} = m^2 \quad ; \quad \frac{z - y}{2} = n^2$$

pour m et n des entiers positifs premiers entre eux. En reportant dans l'équation, il vient $x^2 = 4m^2n^2$ puis $x = 2mn$ (puisque x est supposé positif).

Finalement m et n sont de parité contraire, car sinon y et z seraient tous deux pairs. □

On est maintenant prêt pour donner la descente infinie faite par Fermat pour prouver qu'il n'existe aucun triplet (x, y, z) d'entiers strictement positifs tels que $x^4 + y^4 = z^4$. En réalité, on prouve un résultat légèrement plus fort : il n'existe pas d'entiers x, y et z strictement positifs tels que $x^4 + y^4 = z^2$.

Supposons qu'un tel triplet existe. Déjà on peut supposer que x, y et z sont premiers entre eux dans leur ensemble, sinon on obtient directement une solution plus petite en divisant par le PGCD. Dans ces conditions, en appliquant le théorème précédent, et quitte à échanger les rôles de x et de y, il existe des entiers m et n premiers entre eux tels que :

$$x^2 = 2mn \quad ; \quad y^2 = m^2 - n^2 \quad ; \quad z = m^2 - n^2$$

La deuxième égalité fournit $m^2 = n^2 + y^2$ et les entiers m, n et y sont premiers entre eux dans leur ensemble. En outre, y est impair (puisque x est pair), et donc le théorème précédent s'applique et donne l'existence d'entiers u et v premiers entre eux tels que :

$$n = 2uv \quad ; \quad y = u^2 - v^2 \quad ; \quad m = u^2 + v^2$$

On obtient $x^2 = 2mn = 4uv\,(u^2 + v^2)$. Si d est un diviseur commun de u et de $u^2 + v^2$, il divise v^2 et donc vaut 1 puisque u et v sont premiers entre eux. Ainsi les nombres u, v et $u^2 + v^2$ sont premiers entre eux deux à deux et leur produit est un carré. Chacun d'eux est alors un carré et il existe des entiers x', y' et z' tels que :

$$u = x'^2 \quad ; \quad v = y'^2 \quad ; \quad u^2 + v^2 = z'^2$$

On tire directement de là $x'^4 + y'^4 = z'^2$ et donc une nouvelle solution.

D'autre part, on a l'argument de descente :

$$z' \leqslant z'^2 = m < m^2 + n^2 = z$$

l'inégalité stricte résultant du fait que $n > 0$ (x étant supposé non nul).

Cela conclut la preuve.

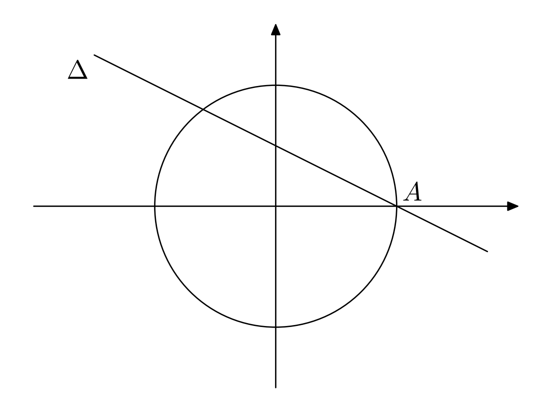
4.4 Équations de degré 2

Il est important de noter que l'on a des méthodes assez générales pour déterminer toutes les solutions rationnelles d'une équation de degré 2 ayant deux inconnues.

Nous allons présenter la méthode sur un exemple simple. Supposons que l'on ait à déterminer les rationnels x et y tels que :

$$x^2 + y^2 = 1$$

Autrement dit, on cherche à trouver tous les points à coordonnées rationnelles sur le cercle unité. Pour cela, il nous faut déjà connaître un point particulier A (à coordonnées rationnelles) sur le cercle : ici, c'est facile, on prend celui de coordonnées $(1, 0)$ par exemple. Si l'on trace une droite Δ (non verticale) passant par A, elle recoupe le cercle en un point B.



Le fait est que le point B est à coordonnées rationnelles si, et seulement si la pente de la droite est rationnelle. En effet, si Δ n'est pas verticale, une équation de Δ est de la forme $y = t\,(x - 1)$. Les points d'intersection de Δ et du cercle vérifient donc le système d'équation :

$$\begin{gathered} x^2 + y^2 = 1 \\ y = t\,(x - 1) \end{gathered}$$

ce qui nous donne :

$$x^2 + t^2\,(x - 1)^2 = 1$$

ou encore :

$$\left(1 + t^2\right) x^2 - 2xt^2 + \left(t^2 - 1\right) = 0$$

Cette équation admet à l'évidence $x = 1$ comme solution (puisque A est un point commun à Δ et au cercle) et la somme des deux racines est donnée par $\frac{2t^2}{1+t^2}$. L'autre racine vaut donc :

$$x = \frac{t^2 - 1}{t^2 + 1}$$

Le y correspondant est donné *via* la formule $y = t(x - 1) = \frac{-2t}{t^2+1}$. Ces deux nombres sont bien rationnels si t l'est.

Réciproquement, il est clair que si les points A et B (distincts) sont à coordonnées rationnelles, la pente de la droite (AB) est rationelle. Ainsi, on a prouvé que toutes les solutions rationnelles, hormis la solution $x = 1$, $y = 0$ sont données par les formules :

$$x = \frac{t^2 - 1}{t^2 + 1} \quad ; \quad y = \frac{-2t}{1 + t^2}$$

Avant de continuer, remarquons que cela donne une nouvelle preuve du théorème 4.3.1. En effet, si x, y et z sont solutions de $x^2 + y^2 = z^2$, on obtient :

$$\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1$$

et on applique la résolution obtenue précédemment.

Notons que dans le cas général d'une équation de degré 2, on n'a plus forcément affaire à un cercle, mais à une conique (qui peut-être soit une ellipse, soit une parabole, soit une hyperbole). Toutefois la méthode se généralise mot pout mot : on trouve une solution particulière, puis on regarde l'intersection de la conique avec les droites de pente rationnelle passant par cette solution. On obtient ainsi toutes les solutions rationnelles de l'équation.

Application à la descente infinie

Les idées précédentes s'appliquent encore, du moins partiellement, lorsque l'équation fait intervenir un plus grand nombre de variables mais que certaines d'entre elles apparaissent en degré inférieur ou égal à 2. On isole alors ces variables en considérant les autres comme paramètres et on résout l'équation comme on l'a expliqué dans le paragraphe précédent.

Cette méthode ne permet pas en général de trouver directement toutes les solutions rationnelles de l'équation, mais permet à partir de l'une d'entre elles d'en construire une nouvelle. Elle peut donc être utilisée lors d'une descente infinie pour prouver qu'une équation donnée n'a pas de solution. Ou, au contraire, elle peut aussi permettre de prouver qu'une équation a une infinité de solutions : on part de l'une d'entre elles qui saute aux yeux, à partir de celle-ci on en construit une nouvelle, puis une autre, et ainsi de suite. Il faut finalement prouver que toutes les solutions obtenues sont distinctes mais c'est souvent le cas.

Équation de Pell-Fermat

L'équation de Pell-Fermat est la suivante :

$$x^2 - dy^2 = \pm 1$$

où d est un entier que l'on suppose sans facteur carré.

Intéressons-nous en premier lieu à l'équation :

$$x^2 - dy^2 = 1$$

Pour la résoudre on peut être tenté d'appliquer la méthode vue précédemment. On constate que le couple $(1, 0)$ est toujours solution. On introduit donc un nombre rationnel t tel que $y = t\,(1 - x)$. L'équation devient alors :

$$x^2 - dt^2\,(1 - x)^2 = 1$$

et la seconde solution de cette équation est :

$$x = \frac{dt^2 + 1}{dt^2 - 1}$$

ce qui nous donne :

$$y = \frac{-2t}{dt^2 - 1}$$

On a ainsi déterminé toutes les solutions rationnelles. Si l'on s'intéresse désormais aux solutions entières, il faut se demander pour quels rationnels $t = \frac{a}{b}$, les fractions x et y sont entières, c'est-à-dire pour quels entiers a et b, $da^2 - b^2$ divise $da^2 + b^2$. Le PGCD de ces deux nombres divise $2da^2$ et $2b^2$ qui est un diviseur de $2d$ puisque a et b et donc a^2 et b^2 sont premiers entre eux.

Donc, déjà dans le cas où $d = 2$, on est ramené à déterminer les entiers a et b pour lesquels le dénominateur $da^2 - b^2$ est un diviseur de 4... et on revient ainsi presque à la case départ.

Nous voyons sur cet exemple que la méthode des équations de degré 2 si elle fonctionne sans bavure pour les solutions rationnelles, peut être mise en défaut si l'on ne recherche que les solutions entières.

Toutefois, on peut résoudre l'équation de Pell-Fermat et plus précisément, on a le théorème suivant :

Théorème 4.4.1 *Soit d un entier sans facteurs carrés. L'équation (que l'on cherche à résoudre en entiers positifs) :*

$$x^2 - dy^2 = 1$$

admet toujours au moins une solution. Notons (x_0, y_0) une solution non nulle pour laquelle $x_0 + y_0\sqrt{d}$ est minimal. Une telle solution s'appelle une solution fondamentale.

Les autres solutions de l'équation sont les couples (x_n, y_n) définis par :

$$x_n + y_n\sqrt{d} = \left(x_0 + y_0\sqrt{d}\right)^n$$

pour tout entier relatif n.

Démonstration. Nous allons admettre dans cette preuve l'existence d'une solution non triviale (c'est-à-dire pour laquelle $x_0 \neq 0$ et $y_0 \neq 0$) et donc l'existence d'une solution fondamentale. Cette existence est prouvée dans le second tome, dans le chapitre sur les fractions continues.

Ensuite, il est facile de voir que x_n et y_n définis par :

$$x_n + y_n\sqrt{d} = \left(x_0 + y_0\sqrt{d}\right)^n$$

forment toujours une solution. En effet, on multiplie par la quantité conjuguée pour obtenir :

$$x_n^2 - dy_n^2 = \left(x_0^2 - dy_0^2\right)^n = 1$$

Montrons que ces solutions sont les seules. La méthode consiste à partir d'une solution (x, y). On considère le nombre $x + y\sqrt{d}$ et on veut le diviser par $x_0 + y_0\sqrt{d}$:

$$\frac{x + y\sqrt{d}}{x_0 + y_0\sqrt{d}} = \left(x + y\sqrt{d}\right)\left(x_0 - y_0\sqrt{d}\right) = (xx_0 - dyy_0) + (yx_0 - xy_0)\sqrt{d}$$

Comme $x_0 + y_0\sqrt{d} > 1$, on a $(xx_0 - dyy_0) + (yx_0 - xy_0)\sqrt{d} < x + y\sqrt{d}$. D'autre part, les couples (x_0, y_0) et (x, y) sont solutions de l'équation, et donc on a :

$$\left(\frac{x_0}{y_0}\right)^2 = d + \frac{1}{y_0^2} \quad ; \quad \left(\frac{x}{y}\right)^2 = d + \frac{1}{y^2}$$

et comme $y > y_0$ et $d > 1$, il vient $yx_0 - xy_0 \geqslant 0$ et $xx_0 - dyy_0 \geqslant 0$. On obtient par le fait une solution plus petite.

À ce niveau, on a tous les éléments pour conclure et on laisse le lecteur le faire proprement.
□

4.5 Équations de degré 3

Certaines méthodes du paragraphe précédent s'appliquent encore aux équations de degré 3. Supposons donné un polynôme à deux variables $P(x, y)$ ne faisant intervenir que des termes dont le degré total est inférieur à 3 et intéressons à l'équation diophantienne :

$$P(x, y) = 0$$

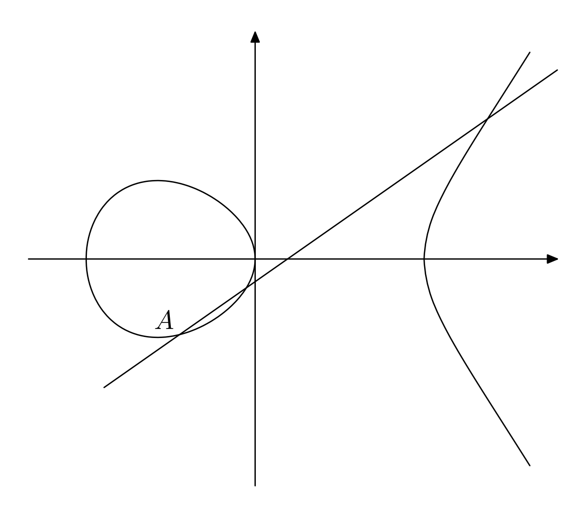
dont on cherche au choix les solutions entières ou rationnelles.

Dans cette situation, il est bien plus difficile de donner une méthode générale pour déterminer toutes les solutions, mais il reste possible, dans certains cas, de construire à partir de nouvelles solutions à partir d'anciennes. Là encore, cela peut se combiner fructueusement à une descente infinie ou permettre de montrer qu'une équation donnée admet une infinité de solutions.

Voyons comment on fait la construction sur un exemple. Supposons que l'équation diophantienne soit la suivante :

$$y^2 = x^3 - 5x$$

et donc $P(x,y) = y^2 - x^3 + 5x$. On cherche des points à coordonnées rationnelles sur la courbe[6] donnée par cette équation :



On commence par trouver un point évident sur la courbe. Ici, le point A de coordonnées $x = 1$, $y = -2$ convient. Si l'on trace une droite passant par A, et que l'on cherche les autres intersections de cette droite avec la courbe, on va être amené à résoudre une équation de degré 2 qui donc à toutes les chances de faire intervenir des racines carrées dans sa résolution. Ce n'est pas agréable.

Il y a deux moyens de contourner ce problème. Le premier est de considérer une droite qui passent par *deux* points à coordonnées rationnelles de la courbe. Le troisième point d'intersection sera donné par une équation de degré 1 et donc à coordonnées rationnelles. Cependant, cela nécessite de connaître deux points de la courbe.

Le second moyen, que nous allons illustrer ici, est de choisir une droite particulière passant par le point A, en l'occurrence la tangente à la courbe. L'équation de la tangente[7] est (de façon très générale) donnée par la formule :

$$\frac{\partial P}{\partial x}(x_0, y_0) \cdot (x - x_0) + \frac{\partial P}{\partial y}(x_0, y_0) \cdot (y - y_0) = 0$$

où x_0 et y_0 sont les coordonnées du point duquel on cherche la tangente (et où $\frac{\partial P}{\partial x}$ désigne la dérivée du polynôme P par rapport à la variable x, et donc en supposant y constant). Ici $x_0 = -1$ et $y_0 = -2$. On calcule les dérivées partielles et on obtient :

$$\frac{\partial P}{\partial x}(x, y) = -3x^2 + 5 \quad ; \quad \frac{\partial P}{\partial y}(x, y) = 2y$$

Par application de la formule, on voit que la tangente à la courbe en A a pour équation :

$$2(x+1) = 4(y+2)$$

[6]Une courbe donnée par une équation de degré 3 est appelée une *cubique*.

[7]Il se peut que la formule donnée n'aboutisse pas à une véritable équation de droite, lorsque les deux coefficients $\frac{\partial P}{\partial x}(x_0, y_0)$ et $\frac{\partial P}{\partial y}(x_0, y_0)$ sont simultanément nuls. Dans ce cas, on dit que le point (x_0, y_0) est *singulier*. Un point qui n'est pas singulier est dit *régulier*. Une courbe d'équation $y^2 = x^3 + ax + b$ (avec a et b réels) dont tous les points sont réguliers est appelée une *courbe elliptique*.

soit encore :

$$y = \frac{1}{2}x - \frac{3}{2}$$

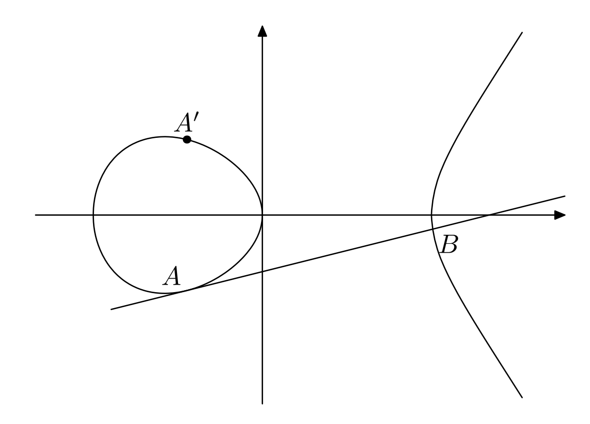
En reportant désormais dans l'équation diophantienne, on obtient l'équation polynômiale :

$$x^3 - \frac{1}{4}x^2 - \frac{7}{2}x - \frac{9}{4} = 0$$

Elle admet évidemment (-1) comme racine puisque la tangente passe par le point A. Mais en réalité la racine (-1) est double (ceci est justement lié à la condition de tangence). Le polynôme se factorise donc par $(x+1)^2$ et la troisième solution est rationnelle :

$$x = \frac{9}{4}$$

Le y correspondant est $-\frac{3}{8}$. On a ainsi construit une seconde solution de l'équation. Graphiquement, on a :



Désormais on a deux points à coordonnées rationnelles sur la courbe. Cependant la droite droite (AB) ne recoupe pas la courbe, puisque A est point d'intersection double. Mais on peut regarder la droite $(A'B)$ où A' est le symétrique de A par rapport à l'axe des abscisses par exemple. On peut également si l'on préfère considérer la tangente en B qui elle aussi, comme précédemment, fournit un nouveau point. De cette façon, on obtient une infinité de solutions rationnelles à l'équation diophantienne de départ.

Notons que parfois cette méthode est inefficace. Par exemple si l'on considère l'équation $y^2 = x^3 - x$ et que l'on essaie de faire la construction en partant de la solution $x_0 = 1$, $y_0 = 0$ par exemple, l'équation de la tangente sera $x = 1$, ce qui ne fournit pas de nouvelles solutions (le problème étant que les termes en x^3 se sont simplifiés).

4.6 Exercices

Exercice 167 **a)** Prouver que le produit de deux entiers consécutifs n'est jamais un carré parfait non nul.

b) Prouver que le produit de trois entiers consécutifs n'est jamais un carré parfait non nul.

c) Prouver que le produit de quatre entiers consécutifs n'est jamais un carré parfait non nul.

Exercice 168 Trouver tous les rationnels x et y vérifiant :

$$x^2 + 3y^2 = 1$$

Exercice 169 **a)** Trouver tous les entiers n et a strictement positifs tels que $5^n = a^2$.
b) Trouver tous les entiers n et a strictement positifs tels que $5^n = a^2 - 1$.
c) Trouver tous les entiers n et a strictement positifs tels que $5^n = a^2 - 2$.

Exercice 170* (France 02) On considère 2002 rationnels $x_1, \ldots, x_{2002}$ tels que, pour tout sous-ensemble I de $\{1, \ldots, 2002\}$ de cardinal 7, il existe un sous-ensemble J de $\{1, \ldots, 2002\}$ de cardinal 11 vérifiant :

$$\frac{1}{7}\sum_{i\in I} x_i = \frac{1}{11}\sum_{j\in J} x_j$$

Prouver que tous les x_i sont égaux.

Exercice 171* (Biélorussie 99) Prouver qu'il existe une infinité de triplets de rationnels non entiers positifs (x, y, z) tel que :

$$\left\{x^3\right\} + \left\{y^3\right\} = \left\{z^3\right\}$$

où $\{t\} = t - [t]$ désigne la partie décimale de t.

Exercice 172* Quelle est la valeur minimale positive de $12^m - 5^n$ pour m et n des entiers strictements positifs.

Exercice 173* (Hongrie 98) Trouver tous les entiers strictement positifs x, y et z tels que $z \geqslant 2$ et :

$$(x+1)^2 + \ldots + (x+99)^2 = y^z$$

Exercice 174* Montrer que tout entier relatif peut s'écrire comme la somme de cinq cubes d'entiers relatifs d'une infinité de manières différentes.

Exercice 175* Trouver tous les entiers strictement positifs x et y tels que $x^y = y^x$.

Exercice 176* (Irlande 96) Soient p un nombre premier et a et b des entiers positifs. Prouver que si $2^p + 3^p = a^n$, alors $n = 1$.

Exercice 177* (Lituanie 94) Trouver les entiers m, n et k tels que $k \geqslant 2$ et :

$$1 + 2! + 3! + \ldots + n! = m^k$$

Exercice 178* (Italie 94) Trouver tous les entiers x et y pour lesquels :

$$y^2 = x^3 + 16$$

Exercice 179* (OIM 81) Soient m et n deux entiers ($1 \leqslant m \leqslant 1981$ et $1 \leqslant n \leqslant 1981$) vérifiant :

$$\left(n^2 - mn - m^2\right)^2 = 1$$

Déterminer le maximun de $m^2 + n^2$.

Exercice 180* (Putnam 73) Un fermier possède un troupeau de 1973 vaches. Chaque vache a une masse qui est un nombre entier, et chaque fois que l'on retire une vache du troupeau, on peut séparer le groupe restant en deux groupes de 986 vaches de masse égale. Montrer que toutes les vaches du troupeau ont la même masse.

Exercice 181* (Saint Petersbourg 97) Soient x, y et z des entiers strictement positifs tels que $2x^x + y^y = 3z^z$. Prouver que $x = y = z$.

Exercice 182* (Irlande 95) Pour quelles valeurs de a l'équation :

$$x^2 + axy + y^2 = 1$$

admet-elle une infinité de solutions dans $\mathbf{Z}$?

Exercice 183* (Afrique du sud 95) Soit x et y des entiers positifs tels que :

$$A = \frac{x^2 + y^2 + 1}{xy}$$

est entier. Montrer que $A = 3$.

Exercice 184* (Bac 2003) Trouver tous les entiers x, y et z tels que :

$$x^2 + y^2 = 7z^2$$

Exercice 185* (Kömal) Trouver tous les entiers relatifs a et b tels que $a^4 + (a+b)^4 + b^4$ soit un carré parfait.

Exercice 186* (CG 90) a) Trouver trois nombres entiers naturels a, b, c distincts ou non, tels que :

$$\frac{1}{4} = \frac{1}{a^2} + \frac{1}{b^2} + \frac{1}{c^2}$$

b) Déterminer tous les entiers naturels n tels qu'il existe n nombres entiers naturels $x_1, \ldots, x_n$ distincts ou non, vérifiant :

$$1 = \frac{1}{x_1^2} + \frac{1}{x_2^2} + \ldots + \frac{1}{x_n^2}$$

Exercice 187* (SL 83) Trouver tous les entiers relatifs x pour lesquels $1 + x + x^2 + x^3 + x^4$ est un carré.

Exercice 188** Trouver tous les entiers positifs ou nuls a, b, c et d vérifiant :

$$a^2 + 5b^2 - 2c^2 - 2cd - 3d^2 = 0$$

Exercice 189 (Putnam 76)** Trouver tous les nombres premiers p, q et les entiers $r, s \geqslant 2$ vérifiant :

$$|p^r - q^s| = 1$$

Exercice 190 (SL 02)** Quel est le plus petit entier t pour lequel il existe des entiers $x_1, \ldots, x_t$ vérifiant :

$$x_1^3 + \ldots + x_t^3 = 2002^{2002}$$

Exercice 191** Trouver tous les entiers x et y vérifiant :

$$y^2 = x^3 - 3x + 2$$

Exercice 192 (Taïwan 98)** Existe-t-il une solution de :

$$x^2 + y^2 + z^2 + u^2 + v^2 = xyzuv - 65$$

avec x, y, z, u et v des entiers supérieur à 1998 ?

Exercice 193 (Inde 98)** Trouver tous les entiers strictement positifs x, y et n tels que $\text{PGCD}(x, n+1) = 1$ et :

$$x^n + 1 = y^{n+1}$$

Exercice 194 (OIM 97)** Trouver tous les couples (a, b) d'entiers $a \geqslant 1$, $b \geqslant 1$ vérifiant l'équation :

$$a^{b^2} = b^a$$

Exercice 195 (OIM 88)** Soient a et b deux entiers strictement positifs tels que $ab + 1$ divise $a^2 + b^2$. Montrer que $\frac{a^2+b^2}{ab+1}$ est un carré parfait.

Exercice 196 (Équation de Markov)** Pour quels entiers positifs ou nuls n l'équation :

$$a^2 + b^2 + c^2 = nabc$$

admet-elle une solution en entiers strictement positifs ?

Exercice 197 (Biélorussie 00)** On considère l'équation :

$$(a^a)^n = b^b \quad (\star)$$

a) Pour quelles valeurs de n, $(\star)$ admet-elle une solution avec $a, b > 1$.
b) Résoudre $(\star)$ pour $n = 5$.

Exercice 198* (SL 95)** Trouver tous les entiers strictement positifs x et y tels que :

$$x + y^2 + z^3 = xyz$$

où $z = \text{PGCD}(x, y)$.

Exercice 199* (Fermat) a)** Trouver tous les triangles rectangles à côtés entiers dont l'aire est le carré d'un nombre entier.

b) Trouver tous les entiers positifs x, y et z vérifiant :

$$x^4 - y^4 = z^2$$

Exercice 200** (Moscou 99)** Trouver tous les entiers n, k, ℓ, m tels que $\ell > 1$ et :

$$\left(1 + n^k\right)^\ell = 1 + n^m$$

5 Corrigé des exercices

5.1 Exercices de « *Premiers concepts* »

Solution de l'exercice 1 : On sait que si la décomposition en facteurs premiers de n est :

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

alors $d(n)$ est donné par la formule :

$$d(n) = (\alpha_1 + 1) \cdots (\alpha_k + 1)$$

Ce dernier nombre est impair si, et seulement si chacun des facteurs est impair, c'est-à-dire si, et seulement si α_i est pair pour tout i. Ceci est bien équivalent au fait que n soit un carré.

Solution de l'exercice 2 : On remarque que :

$$3\left(3^{n-1} + 5^{n-1}\right) < 3^n + 5^n < 5\left(3^{n-1} + 5^{n-1}\right)$$

et donc le quotient $\frac{3^n+5^n}{3^{n-1}+5^{n-1}}$ supposé entier ne peut valoir que 4. L'égalité donne $3^{n-1} = 5^{n-1}$ et la seule solution est obtenue pour $n = 1$.

Solution de l'exercice 3 : Nous allons montrer qu'il est multiple de 2 et de 3. Comme 2 et 3 sont premiers entre eux, cela conclura. La factorisation :

$$n^3 - n = n\left(n^2 - 1\right) = n(n-1)(n+1)$$

nous montre que $n^3 - n$ s'écrit comme le produit de trois nombres consécutifs. Parmi eux, il y a forcément un multiple de 2 et un multiple de 3 (pas forcément distincts bien sûr). Le produit est donc à la fois multiple de 2 et de 3 comme on le voulait.

Solution de l'exercice 4 : Il suffit de remarquer que :

$$3(14n + 3) - 2(21n + 4) = 1$$

Le théorème de Bézout assure que numérateur et dénominateur de la fraction sont premiers entre eux et donc qu'elle est irréductible.

Solution de l'exercice 5 : Cela résulte directement des formules :

$$\begin{aligned} 5x + 2 &= 8(2x + 3) - 11(x + 2) \\ 2x + 3 &= 7(5x + 2) - 11(3x + 1) \end{aligned}$$

Solution de l'exercice 6 : On factorise $p^2 - 1 = (p-1)(p+1)$. Comme p est un nombre premier différent de 2, il est impair. Ainsi $p-1$ et $p+1$ sont tous les deux pairs et le produit est un multiple de 4.

De même $p > 3$ et donc p ne peut-être un multiple de 3. On en déduit que soit $p-1$, soit $p+1$ est un multiple de 3, et donc $p^2 - 1$ en est également un.

En conclusion, $p^2 - 1$ est multiple de 3 et de 4, et donc de 12.

Solution de l'exercice 7 : Soit p un nombre premier. L'hypothèse nous dit que $nv_p(a) \geqslant (n+1)\, v_p(b)$, soit encore :

$$v_p(a) \geqslant \left(1+\frac{1}{n}\right) v_p(b)$$

et par passage à la limite $v_p(a) \geqslant v_p(b)$ pour tout nombre premier p. On en déduit que a divise b.

Solution de l'exercice 8 : La décomposition en facteurs premiers nous donne :

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

pour certains nombres premiers p_i distincts deux à deux et certains exposants α_i strictement positifs. On a $p_i \geqslant 2$ et donc *a fortiori* $p_i^{\alpha_i} \geqslant 2$. On en déduit que $n \geqslant 2^k$ et puis l'inégalité proposée en prenant les logarithmes.

Solution de l'exercice 9 : Comme p divise n^k, on a $v_p(n^k) > 0$ et en particulier $v_p(n) = \frac{1}{k} v_p(n^k) > 0$. On en déduit que p divise n.

Solution de l'exercice 10 : Notons a le plus petit élément de X et b le deuxième plus petit (et donc $b > 1$). D'après l'hypothèse, il existe $k \in X$ tel que $b = ak^2$. Il est évidemment que l'on ne peut pas avoir $k \geqslant b$, c'est donc que $k = a$ puis $b = a^3$. Notons qu'alors $a \neq 1$ puisque $b \neq a$.

Supposons que X contienne un autre élément c que l'on choisit encore minimal. Encore d'après l'hypothèse, il doit exister k et k' dans X tels que $c = ak^2$ et $c = bk'^2 = a^3 k'^2$. De là, on déduit que $ak^2 = a^3 k'^2$ puis $(ak')^2 = k^2$ et finalement $ak' = k$.

Par ailleurs, les entiers k et k' sont deux éléments de X avec $k' < k$, donc à appliquant une nouvelle fois l'hypothèse, il doit exister $k'' \in X$ tel que $k = k'k''^2$. On en déduit que $a = k''^2$ et donc que, puisque $a > 1$, il vient $k'' < a$. Cela contredit la minimalité de a.

On en déduit que X est réduit à $\{a, a^3\}$ puis que les ensembles de cette forme sont les seules solutions.

Solution de l'exercice 11 : Comme n est un multiple de 18, il s'écrit :

$$n = 2^\alpha 3^\beta \prod_i p_i^{\gamma_i}$$

pour certains entiers $\alpha \geqslant 1$, $\beta \geqslant 2$ et $\gamma_i \geqslant 0$, et pour certains nombres premiers $p_i \geqslant 5$ deux à deux distincts. D'autre part on constate que 18 a exactement 6 diviseurs (qui sont 1, 2, 3, 6, 9 et 18). Comme un diviseur de 18 doit être un diviseur de n, on a forcément $d_1 = 1$, $d_2 = 2$, $d_3 = 3$, $d_4 = 6$, $d_5 = 9$ et $d_6 = 18$. En particulier, 4 ne divise pas n et $\alpha = 1$.

Le nombre de diviseurs de n est donné par la formule :

$$2\,(\beta+1) \prod_i (\gamma_i + 1)$$

Ce nombre doit faire 16 et comme $\beta + 1 \geqslant 3$, les seules solutions sont $\beta = 3$ (et $\gamma_1 = 1$) et $\beta = 7$ (et $\gamma_1 = 0$). Les éventuelles solutions sont donc, soit 2×3^7, soit $2 \times 3^2 \times p$ pour un nombre premier $p \geqslant 19$.

On calcule les diviseurs successifs de 2×3^7 : $d_7 = 27$, $d_8 = 54$, $d_9 = 81$. On a $d_9 - d_8 > 17$ et ce nombre n'est donc pas solution.

De même, on calcule les diviseurs de $2 \times 3^2 \times p$. Si $19 \leqslant p < 27$, on a $d_7 = p$, $d_8 = 27$, $d_9 = 2p$, ce qui fournit l'équation $2p - 27 = 17$ et donc $p = 22$ qui n'est pas premier. Si $27 < p < 54$, on a $d_7 = 27$, $d_8 = p$, $d_9 = 54$ et donc $54 - p = 17$ puis $p = 37$, qui convient. Si $p > 54$, on a $d_7 = 27$, $d_8 = 54$, $d_9 = p$, ce qui donne $p = 71$.

Finalement, il y a deux solutions : $n = 2 \times 3^3 \times 37 = 1998$ et $n = 2 \times 3^3 \times 71 = 3834$.

Solution de l'exercice 12 : Un diviseur commun à a et à b doit diviser $bc - 1$ et donc 1. Ainsi a et b sont premiers entre eux. De même, a, b et c sont premiers entre eux deux à deux.

Si a divise $bc - 1$, il divise également $bc + ac + ab - 1$. De même, b et c doivent diviser $bc + ac + ab - 1$. Comme a, b et c sont premiers entre eux deux à deux, on en déduit que abc divise $ab + bc + ca - 1$. Le quotient :

$$\frac{ab + bc + ca - 1}{abc} = \frac{1}{a} + \frac{1}{b} + \frac{1}{c} - \frac{1}{abc}$$

est inférieur ou égal à $\frac{3}{2}$. Il ne peut donc valoir que 1.

On est amené à résoudre :

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} - \frac{1}{abc} = 1$$

On ne peut pas avoir a, b et c supérieurs ou égaux à 3. Sans perte de généralité, on peut supposer $a \leqslant b \leqslant c$, et donc $a \leqslant 3$ et donc $a = 2$ ou $a = 3$. Si $a = 2$, l'équation devient :

$$\frac{1}{b} + \frac{1}{c} - \frac{1}{2bc} = \frac{1}{2}$$

et comme précédemment b et c ne peuvent pas être simultanément supérieurs ou égaux à 4. On a donc $b = 2$ ou $b = 3$. Pour $b = 2$, l'équation n'a pas de solution en c. Pour $b = 3$, on obtient $c = 5$. On vérifie que le triplet $(2, 3, 5)$ est solution.

De même, on traite le cas $a = 3$. L'équation devient alors :

$$\frac{1}{b} + \frac{1}{c} - \frac{1}{3bc} = \frac{2}{3}$$

Ici, on ne peut avoir b et c supérieurs ou égaux à 3 et comme ils sont supposés supérieurs à a, il n'y a pas de solution.

Finalement, les solutions sont le triplet $(2, 3, 5)$ et toutes ses permutations.

Solution de l'exercice 13 : On sait qu'il existe un nombre premier p qui est tel que tous les nombres $p + 1, \ldots, p + n$ soient composés.

Xavier peut alors tester les entiers de l'ensemble $\{1, \ldots, n - 1\}$ les uns après les autres. Pour tester 1, il propose le nombre $p - 1$: si Pierre répond oui, alors le nombre choisi est 1, sinon ce n'est pas 1. Ensuite, il teste 2 et proposant le nombre $p - 2$, et ainsi de suite.

Il arrive donc à conclure en moins de $n - 1$ questions, puisqu'il est inutile de tester $n - 1$: si aucun des nombres $p - k$ n'est premier pour $k \leqslant n - 2$, c'est donc que c'est $m = n - 1$.

Solution de l'exercice 14 : Notons p, q, ℓ les trois nombres premiers en question. Si leurs racines cubiques étaient dans une même progression arithmétique de raison r, il existerait des entiers m et n non nuls et distincts tels que :

$$\sqrt[3]{p} - \sqrt[3]{q} = mr \quad \text{et} \quad \sqrt[3]{p} - \sqrt[3]{\ell} = nr$$

On a donc :

$$\sqrt[3]{p} - \sqrt[3]{\ell} = \frac{n}{m}\left(\sqrt[3]{p} - \sqrt[3]{q}\right)$$

et donc il existe des rationnels non nuls α et β tels que :

$$\alpha\sqrt[3]{p} + \beta\sqrt[3]{q} = \sqrt[3]{\ell}$$

En élevant au cube, il vient donc :

$$\begin{aligned} \ell &= \alpha^3 p + \beta^3 q + 3\alpha\beta(\alpha\sqrt[3]{p} + \beta\sqrt[3]{q})\sqrt[3]{pq} \\ &= \alpha^3 p + \beta^3 q + 3\alpha\beta\sqrt[3]{pq\ell} \end{aligned}$$

Il en résulte que $t = \sqrt[3]{pq\ell}$ est rationnel. Mais on doit avoir $v_p(t^3) = 3v_p(t) = 1$, ce qui est absurde.

Solution de l'exercice 15 : **a)** Oui. Les entiers 7 et 12 sont premiers entre eux, donc d'après le théorème de Bézout, il existe des entiers u et v tels que $7u + 12v = 1$. On a alors :

$$x = x^{7u+12v} = \left(x^7\right)^u \times \left(x^{12}\right)^v$$

Ainsi x s'écrit comme un produit de nombres rationnels. Il est donc rationnel.

Remarque. Le raisonnement précédent ne permet pas de déduire que si x^7 et x^{12} sont entiers, alors x est forcément entier : en effet, parmi u et v il y a au moins un nombre négatif et donc le produit $(x^7)^u \times (x^{12})^v$ cache en réalité un quotient. Toutefois le résultat est quand même vrai. On vient de prouver que x est rationnel, et on sait que x^7 est entier. Un résultat du cours prouve alors que x est entier.

b) Non. Cette fois-ci les entiers 9 et 12 ne sont pas premiers entre eux : leur PGCD est 3. On chosit x irrationnel tel que x^3 est rationnel (par exemple $x = \sqrt[3]{3}$). Alors $x^9 = (x^3)^3$ est bien rationnel, ainsi que $x^{12} = (x^3)^4$.

Solution de l'exercice 16 : En écrivant la valuation 2-adique des deux membres de l'équation, il vient :

$$[x]v_2(x) = -1$$

ce qui impose $[x] = \pm 1$. Si $[x] = 1$, on a $1 \leqslant x < 2$ et donc $x^{[x]} < 2$ ce qui est incompatible avec l'équation. Si $[x] = -1$, x est négatif et $x^{[x]}$ aussi, ce qui est encore incompatible.

Solution de l'exercice 17 : La condition est équivalente à $x + 1$ à la fois multiple de 2, de 3, et ainsi de suite jusqu'à 9. Elle est donc également équivalente à $x + 1$ multiple de PPCM $(2, 3, 4, 5, 6, 7, 8, 9) = 2520$. La plus petite solution positive est $x = 2519$.

Solution de l'exercice 18 : On remarque que si d est un diviseur de n alors $\frac{n}{d}$ aussi. L'indexation des diviseurs donne alors $d_i d_{k+1-i} = n$. Donc :

$$d = \sum_{i=1}^{k-1} d_i d_{i+1} = n^2 \sum_{i=1}^{k-1} \frac{1}{d_i d_{i+1}} \leqslant n^2 \sum_{i=1}^{k-1} \left(\frac{1}{d_i} - \frac{1}{d_{i+1}}\right)$$

la dernière inégalité étant obtenue car $d_{i+1} - d_i \geqslant 1$. On en déduit que :

$$d \leqslant n^2 \left(\frac{1}{d_1} - \frac{1}{d_k} \right) = n^2 \left(1 - \frac{1}{n} \right) < n^2$$

Si $n = p$ est un nombre premier, alors $d = p$ qui divise n^2. Si n est composé, alors $k > 2$. Soit p le plus petit diviseur premier de n. On a :

$$d > d_{k-1} d_k = \frac{n^2}{p}$$

et donc :

$$1 < \frac{n^2}{d} < p$$

Mais alors $\frac{n^2}{d}$ est un diviseur de n^2 strictement inférieur à p, ce qui n'est pas possible.

Les seules solutions sont donc les nombres premiers.

<u>*Solution de l'exercice 19*</u> : Soit p un nombre premier impair divisant n. On peut écrire $n = pk$ et :

$$2^{pk} + 1 = \left(2^k + 1\right) \left(2^{k(p-1)} - 2^{k(p-2)} + \cdots + 1\right)$$

Évidemment $1 < 2^k + 1 < 2^{pk} + 1$. On a donc obtenu une factorisation non triviale.

On en déduit que le seul diviseur premier de n est 2 et donc que n est une puissance de 2.

Commentaire. Les nombres de la forme $F_n = 2^{2^n} + 1$ s'appelent les *nombres de Fermat*. Fermat avait conjecturé que tous les nombres de cette forme étaient premiers. C'est le cas de F_0, F_1, F_2, F_3 et F_4. Malheureusement, Euler démontra en 1732 que F_5 est composé. Depuis, on n'a pas trouvé d'autres nombres de Fermat premiers.

<u>*Solution de l'exercice 20*</u> : Soit $n > 1$ un entier. On constate que les entiers 1 et n sont toujours des diviseurs distincts de n et que tous les autres diviseurs de n sont strictement plus petits que n. On en déduit l'inégalité :

$$\sigma(n) \leqslant 1 + n + (d(n) - 2)\, n$$

et cette égalité est stricte dès que n admet plus de deux diviseurs, c'est-à-dire dès que n est composé.

D'autre part, il ne peut y avoir plus de $n - 1$ entiers premiers avec n dans l'intervalle $[1, n]$ (en effet, n n'est pas premier avec lui-même). On en déduit que $\varphi(n) \leqslant n - 1$. En combinant avec l'inégalité obtenue précédemment, on arrive à :

$$\sigma(n) + \varphi(n) \leqslant n \cdot d(n)$$

et cette inégalité est stricte si n est composé.

On en déduit que les seuls n susceptibles de répondre à la question sont les nombres premiers. On vérifie par ailleurs que si p est premier, $d(p) = 2$, $\sigma(p) = p + 1$ et $\varphi(p) = p - 1$, et donc que l'on a bien l'égalité $\sigma(p) + \varphi(p) = p \cdot d(p)$. Les solutions sont donc exactement les nombres premiers.

Solution de l'exercice 21 : Il est clair que cette somme ne possède qu'un nombre fini de termes non nuls, $\left[\frac{n+2^k}{2^{k+1}}\right]$ est nul dès que $2^{k+1} > n + 2^k$, donc $2^k > n$. Cet énoncé se résout facilement si l'on connaît le lemme : pour tout réel x, $[2x] = [x] + \left[x + \frac{1}{2}\right]$ qui se vérifie immédiatement : si $n \leqslant x < n + \frac{1}{2}$, $[x] = n = \left[x + \frac{1}{2}\right]$ et $[2x] = 2n$, et si $n + \frac{1}{2} \leqslant x < n + 1$, $[x] = n$, $\left[x + \frac{1}{2}\right] = n + 1$, et $[2x] = 2n + 1$. Il en résulte que :

$$\left[\frac{n+2^k}{2^{k+1}}\right] = \left[\frac{n}{2^{k+1}} + \frac{1}{2}\right] = \left[\frac{n}{2^k}\right] - \left[\frac{n}{2^{k+1}}\right]$$

La somme s'écrit donc :

$$\left([n] - \left[\frac{n}{2}\right]\right) + \left(\left[\frac{n}{2}\right] - \left[\frac{n}{4}\right]\right) + \left(\left[\frac{n}{4}\right] - \left[\frac{n}{8}\right]\right) + \dots$$

et par « simplification téléscopique », elle vaut $[n]$, soit n si n est un entier.

Solution de l'exercice 22 : Par définition $\pi(p_n) = n$. Ainsi :

$$n \log n = \pi(p_n) \log(\pi(p_n)) \tag{2}$$

D'après le théorème des nombres premiers, le quotient $\pi(p_n) \cdot \frac{\log p_n}{p_n}$ tend vers 1 quand n tend vers l'infini (car p_n tend vers l'infini) et donc en passant au logarithme, il vient :

$$\log(\pi(p_n)) - \log p_n + \log(\log p_n) \to 0$$

puis en divisant tout par $\log p_n$, il vient :

$$\log(\pi(p_n)) \sim \log p_n$$

En appliquant une nouvelle fois le théorème des nombres premiers, la formule (2) donne :

$$n \log n \sim \frac{p_n}{\log p_n} \cdot \log p_n = p_n$$

Solution de l'exercice 23 : Soit E un tel ensemble, et $a \in E$ quelconque. Alors d'après l'hypothèse, $(a + a)/a = 2 \in E$. On peut remarquer que le singleton $\{2\}$ est en fait une solution du problème. On suppose dorénavant que E contient au moins un autre élément que 2.

Si 1 est dans E, alors pour tout $a \in E$, $(a + 1)/1 = a + 1 \in E$, donc une récurrence immédiate montre que $E = \mathbf{N}^*$, qui est bien une solution.

Dans le cas contraire, soit m le plus petit élément de E autre que 2. Si m était pair, disons $m = 2k$ avec $k \geqslant 2$, on aurait $(2k + 2)/2 = k + 1 \in E$. Or $2 < k + 1 < 2k$, ce qui contredirait la minimalité de m. Donc m est impair, et $m + 2$ est aussi dans E, et de même pour $m + 2p$ pour tout $p \geqslant 0$. Tous les nombres impairs à partir de m sont donc dans E, et en particulier km pour tout $k \geqslant 1$ impair. Ainsi, $(km + m)/m = k + 1 \in E$, ce qui montrer que E contient tous les entiers pairs, et en particulier 4. La minimalité de m assure alors que $m = 3$ et donc que E contient tous les entiers au moins égaux à 2, ce qui réciproquement fournit bien une solution au problème.

Finalement, il y a trois solutions, qui sont $\{2\}$, $\mathbf{N}^*$ et $\mathbf{N}^* \setminus \{1\}$.

Solution de l'exercice 24 : On a la factorisation :

$$3^n - 1 = 2\left(3^{n-1} + 3^{n-2} + \cdots + 1\right)$$

Si n est impair le facteur entre parenthèses est une somme de n termes impairs et donc est impair. On en déduit que $3^n - 1$ ne peut être un multiple de 4 et donc *a fortiori* de 2^n pour $n > 1$. Le cas $n = 1$ convient comme on le vérifie à part.

Supposons n pair et posons donc $n = 2k$. La condition se réécrit 2^{2k} divise $3^{2k} - 1 = \left(3^k - 1\right)\left(3^k + 1\right)$. Les deux nombres $3^k - 1$ et $3^k + 1$ sont distants de 2 et donc leur PGCD est un diviseur de 2. D'autre part, ces nombres sont toujours pairs et donc PGCD $\left(3^k - 1, 3^k + 1\right) = 2$. On en déduit que soit $3^k - 1$, soit $3^k + 1$ est divisible par 2^{2k-1}. Cela implique en toutes circonstances $3^k + 1 \geqslant 2^{2k-1}$ ce qui n'est plus vrai pour $k \geqslant 3$. On vérifie à la main que $k = 0$, $k = 1$ et $k = 2$ sont solutions.

Finalement les seules solutions sont $n = 1$, $n = 2$ et $n = 4$.

Solution de l'exercice 25 : Soit p un nombre premier. On va prouver que les valuations p-adiques des deux membres de l'égalité à prouver sont toujours égales. Notons $\alpha = v_p(a)$, $\beta = v_p(b)$ et $\gamma = v_p(c)$. Il s'agit de montrer que :

$$\begin{aligned} &2 \inf(\alpha, \beta, \gamma) - \inf(\alpha, \beta) - \inf(\beta, \gamma) - \inf(\alpha, \gamma) \\ &= 2 \sup(\alpha, \beta, \gamma) - \sup(\alpha, \beta) - \sup(\beta, \gamma) - \sup(\alpha, \gamma) \end{aligned}$$

Comme les rôles de α, β et γ sont similaires, on peut supposer $\alpha \leqslant \beta \leqslant \gamma$ et donc ce cas les deux membres de l'égalité précédentes sont égaux à $-\beta$. Ce qui conclut.

Remarque. On ne peut évidemment pas déduire de ce qui précède que les quotients de l'énoncé sont égaux à $\frac{1}{b}$. Pourquoi ?

Solution de l'exercice 26 : Pour construire une telle décomposition, on utilise l'algorithme glouton : on commence par déterminer le plus grand entier, disons a_k, tel que $\mathrm{C}_{a_k}^k \leqslant n$. Puis, on recommence avec n et k remplacés respectivement par $n - \mathrm{C}_{a_k}^k$ et $k - 1$. Comme, par construction, on a $n < \mathrm{C}_{a_k+1}^k$ c'est donc que :

$$n - \mathrm{C}_{a_k}^k < \mathrm{C}_{a_k}^{k-1}$$

ce qui assure que la suite des a_i est bien strictement décroissante

On prouve maintenant l'unicité. Supposons que n possède deux représentations distinctes associées respectivement aux suites $a_k, \ldots, a_t$ et $b_k, \ldots, b_r$. On considère le plus grand indice pour lequel ces deux suites différent. Quitte à éliminer des termes, on peut supposer que cet indice est k et que $a_k > b_k$. Mais alors :

$$n \leqslant \mathrm{C}_{b_k}^k + \mathrm{C}_{b_{k-1}}^{k-1} + \cdots + \mathrm{C}_{b_k-k+1}^1 < \mathrm{C}_{b_k+1}^k \leqslant \mathrm{C}_{a_k}^k \leqslant n$$

ce qui constitue une contradiction.

Solution de l'exercice 27 : **a)** D'après le principe des tiroirs parmi les a_i, il y en a deux consécutifs, qui sont donc premiers entre eux.

b) Écrivons pour tout i, $a_i = 2^{\alpha_i} b_i$ pour un certain nombre impair b_i, forcément compris entre 1 et $2n$. D'après le principe des tiroirs, puisqu'il y a n nombres impairs entre 1 et $2n$, il existe i et j tels que $b_i = b_j$. On peut supposer $\alpha_i \leqslant \alpha_j$ et dans ce cas a_i divise a_j.

Solution de l'exercice 28 : Si n n'est pas premier, il admet un diviseur d différent de n et supérieur à $\sqrt{n}$. Ainsi, $\sigma(n) - n \geqslant \sqrt{n}$. La suite $\sigma(n_i) - n_i$ est constante, disons égale à k. D'autre part, on prouve par récurrence que $n_i \geqslant i$ pour tout i. Considérons un $i > k^2$. Si n_i n'était pas premier, on aurait :

$$\sigma(n_i) - n_i \geqslant \sqrt{i} > k$$

ce qui est impossible. Ainsi n_i est premier et $k = 1$. On conclut en remarquant que si $\sigma(n) = n + 1$, alors forcément n est un nombre premier.

Solution de l'exercice 29 : Déjà $d_1 = 1$. Si n était impair, tous ses diviseurs seraient impairs et donc $d_1^2 + d_2^2 + d_3^2 + d_4^2 = n$ serait pair. Ce n'est pas possible. Donc n est pair et $d_2 = 2$. Si d_3 et d_4 étaient de même parité, la somme $d_1^2 + d_2^2 + d_3^2 + d_4^2$ serait impaire, ce qui n'est pas possible non plus.

Supposons que 4 divise n. Les nombres d_3 et d_4 sont alors 4 et un nombre premier p à l'ordre près et on est ramené à l'équation :

$$21 + p^2 = n$$

Or p divise n, donc p divise 21 et ainsi p vaut 3 ou 7. On vérifie qu'aucun des deux ne fournit une solution.

Si 4 ne divise pas n, on a $d_3 = p$ où p est le plus petit diviseur impair de n, et $d_4 = 2p$ puisque d_4 doit être pair. L'équation devient :

$$5 + 5p^2 = n$$

Donc p divise 5 puis $p = 5$. Cela conduit à $n = 130$ qui convient.

Solution de l'exercice 30 : Écrivons $a_n + b_n = \alpha + nr$ et $a_n b_n = \beta + ns$ pour des entiers α, β, r et s. Pour tout n, les nombres a_n et b_n sont les racines du polynôme :

$$X^2 - (\alpha + nr) X + (\beta + ns)$$

Le discriminant $\Delta_n = (\alpha + nr)^2 - 4(\beta + ns)$ est donc un carré parfait pour tout entier $n \geqslant 0$. On a l'égalité :

$$r^2 \Delta_n = (nr^2 + \alpha r - 2s)^2 + d$$

où $d = -4s^2 + 4rs\alpha - 4\beta r^2$ est indépendant de n. Si $r \neq 0$, pour n suffisamment grand, on a l'inégalité :

$$(nr^2 + \alpha r - 2s - 1)^2 < r^2 \Delta_n < (nr^2 + \alpha r - 2s + 1)^2$$

Comme $r^2 \Delta_n$ doit être un carré, on doit forcément avoir $r^2 \Delta_n = (nr^2 + \alpha r - 2s)^2$ et donc $d = 0$. Mais alors, notre trinôme admet toujours pour racine $c = \frac{s}{r}$ et donc pour tout n, on a $a_n = c$ ou $b_n = c$.

Solution de l'exercice 31 : En réduisant au même dénominateur, la condition est équivalente à ℓmn divise $(\ell + m + n)(mn + \ell n + \ell m)$. En particulier, ℓ divise $(m + n) mn$ et par le lemme de Gauss ℓ divise $m + n$.

Pareillement m divise $\ell + n$ et n divise $\ell + m$. Les rôles des variables étant symétriques, on peut supposer que n est le plus grand des trois. Du coup, $\ell + m \leqslant 2n$ et la condition de divisibilité impose $\ell + m = n$ ou $\ell + m = 2n$. Dans ce dernier cas, on a forcément $\ell = m = n$ et cette valeur commune est 1 car ils sont premiers entre eux. Le triplet $(1, 1, 1)$ est bien solution.

Sinon, $\ell + m = n$, et en remplaçant, le nombre :

$$2(\ell + m)\left(\frac{1}{\ell} + \frac{1}{m} + \frac{1}{\ell + m}\right)$$

doit être entier, ce qui équivaut à :

$$2(\ell + m)\left(\frac{1}{\ell} + \frac{1}{m}\right) = \frac{2(\ell + m)^2}{lm}$$

est entier. Comme ℓ et m sont premiers entre eux, on peut supposer ℓ impair. Alors ℓ divise $(\ell + m)^2$ et donc divise m^2, ce qui n'est possible que si $\ell = 1$. Alors m divise 2, et $m = 1$ ou $m = 2$.

On déduit de ce qui précède que les solutions sont les triplets $(1, 1, 1)$, $(1, 1, 2)$, $(1, 2, 3)$ et toutes leurs permutations.

Solution de l'exercice 32 : **a)** Décomposons $n > 1$ en facteurs premiers :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_d^{\alpha_d}$$

Les diviseurs d de n pour lesquels $\mu(d) \neq 0$ s'écrivent $d = \prod_{i \in I} p_i$ pour I un certain sous-ensemble de $\{1, \dots, d\}$. La valeur de $\mu(d)$ est alors $(-1)^{\operatorname{Card} I}$.

Pour conclure, il faut donc juste voir que l'ensemble $\{1, \dots, d\}$ possède autant de sous-ensembles de cardinal pair que de sous-ensembles de cardinal impair. Mais à chaque ensemble de cardinal pair, on peut associer un ensemble de cardinal impair en lui ajoutant 1 s'il n'appartient pas à l'ensemble de départ ou en lui otant s'il appartient. Cette association est bijective : il y a donc autant de sous-ensembles de cardinal pair que de cardinal impair, et la formule de sommation est prouvée.

b) La somme proposée se réécrit :

$$\sum_{d|n} \sum_{d'|d} \mu\left(\frac{n}{d}\right) f(d')$$

Dans la somme précédente le terme $f(d')$ apparaît pour tout entier d tel que $d'|d|n$. Ainsi le coefficient qui restera au final de $f(d')$ est :

$$\sum_{d'|d|n} \mu\left(\frac{n}{d}\right)$$

En écrivant $d = d'x$, cette somme s'écrit encore :

$$\sum_{x | \frac{n}{d'}} \mu\left(\frac{n}{d'x}\right) = \sum_{x | \frac{n}{d'}} \mu(x)$$

la dernière égalité provenant du changement de variable $x \mapsto \frac{n}{d'x}$. D'après a), cette somme fait toujours 0 sauf si $\frac{n}{d'} = 1$ (*i.e.* $n = d'$) auquel cas elle fait 1. On trouve ainsi bien la formule annoncée.

Solution de l'exercice 33 : Parmi ces 10 entiers, il y en a 5 impairs. Parmi ces 5 impairs, il y en a au plus 2 qui sont divisibles par 3 (noter que les multiples de 3 sont alternativement pairs et impairs). Parmi ces mêmes 5, il y en a au plus 1 qui est multiple de 5 et au plus 1 multiple de 7.

Donc il y a au moins un des dix entiers qui n'est divisible ni par 2, ni par 3, ni par 5, ni par 7. Appelons-le n. Le PGCD de n et de $n+k$ est un diviseur de k, donc si k est non nul et est compris entre -9 et 9, $\text{PGCD}(n, n+k)$ doit être divisible par un nombre premier strictement inférieur à 10. Mais par construction n n'est divisible par aucun tel nombre premier. L'entier n convient donc.

Solution de l'exercice 34 : Écrivons :

$$\begin{aligned} n &= p_1^{\alpha_1} \cdots p_d^{\alpha_d} \\ m &= p_1^{\beta_1} \cdots p_d^{\beta_d} \end{aligned}$$

où les p_i sont des nombres premiers deux à deux et les exposants α_i et β_i sont des entiers positifs ou nuls.

On a vu dans le cours que le produit des diviseurs de n s'écrit :

$$p_1^{\gamma_1} \cdots p_d^{\gamma_d}$$

pour :

$$\gamma_i = \frac{1}{2}\alpha_i(\alpha_1+1)\cdots(\alpha_d+1)$$

L'hypothèse de l'énoncé assure que pour tout i :

$$\alpha_i(\alpha_1+1)\cdots(\alpha_d+1) = \beta_i(\beta_1+1)\cdots(\beta_d+1)$$

et donc il existe un rationnel q, indépendant de i, telle que $\alpha_i = q\beta_i$. Quitte à intervertir m et n, on peut supposer $q \geqslant 1$. L'hypothèse se réécrit alors :

$$q(q\beta_1+1)\cdots(q\beta_d+1) = (\beta_1+1)\cdots(\beta_d+1)$$

et on voit directement que si $q > 1$, le membre de gauche est strictement supérieur à celui de droite. On a donc $q = 1$ et $m = n$.

Solution de l'exercice 35 : D'après les formules classiques, la somme en question vaut :

$$\frac{(2n+m)(m+1)}{2}$$

et on est donc ramené à l'équation $(2n+m)(m+1) = 2000$. Les nombres $2n+m$ et $m+1$ sont donc des diviseurs associés de 2000. On remarque en outre d'une part que la somme de ces diviseurs vaut $2n+2m+1$ est donc doit être impaire, et d'autre part que $1 < m+1 < 2n+m$.

La décomposition en facteurs premiers de 2000 est $2000 = 2^4 \times 5^3$. En vertu de ce qui précède les seules possibilités sont :

☞ $m+1 = 5$, $2n+m = 400$, soit $m = 4$ et $n = 198$

☞ $m+1 = 25$, $2n+m = 80$, soit $m = 24$ et $n = 28$

☞ $m+1 = 16$, $2n+m = 125$, soit $m = 15$ et $n = 55$

qui effectivement conviennent.

Solution de l'exercice 36 : La condition de l'énoncé assure que pour tout n, on a $\text{PGCD}(a_{2n}, a_n) = \text{PGCD}(2n, n) = n$. Ainsi n divise a_n et on écrit $a_n = nb_n$ pour un entier $b_n > 0$.

Supposons par l'absurde qu'il existe n tel que $b_n > 1$ et soit p un facteur premier de b_n. Comme p divise a_n et a_p, il divise $\text{PGCD}(a_n, a_p) = \text{PGCD}(n, p)$ et donc p divise n. Soit p^a la plus grande puissance de p qui divise n. Alors p^{a+1} divise a_n et puis $\text{PGCD}(a_n, a_{p^{a+1}}) = \text{PGCD}(n, p^{a+1}) = p^a$. C'est une contradiction.

Finalement, $b_n = 1$ pour tout n, et donc $a_n = n$ pour tout n.

Solution de l'exercice 37 : Supposons que n soit composé et que d soit un diviseur strict de n. On peut donc écrire $n = dd'$ et :

$$2^n - 1 = \left(2^d - 1\right)\left(2^{d(d'-1)} + 2^{d(d'-2)} + \cdots + 1\right)$$

Le facteur $2^d - 1$ est non trivial, et donc $2^n - 1$ est composé.

Commentaire. Les nombres de la forme $2^p - 1$ où p est un nombre premier sont appelés *nombres de Mersenne*. On dispose d'algorithmes spécifiques pour tester leur primalité. C'est pourquoi les plus grands nombres premiers connus à ce jour sont des nombres de Mersenne, le plus grand étant :

$$2^{24\,036\,583} - 1$$

découvert le 15 mai 2004.

Solution de l'exercice 38 : Notons n le plus petit multiple de 10 qui apparaît parmi les 39 entiers consécutifs. Il est immédiat que tous les entiers compris entre n et $n+29$ font partie des 39 entiers consécutifs.

Notons s la somme des chiffres de n. Les entiers $n+1, \ldots, n+9$ sont parmi les 39 entiers consécutifs et ont pour somme des chiffres respectivement $s+1, \ldots, s+9$. D'autre part, si on suppose que n ne se termine pas par 90, l'entier $n+19$ est également parmi les 39 entiers consécutifs et a pour somme des chiffres $s+10$. Or, parmi les sommes $s, \ldots, s+10$, il y en a forcément une qui est multiple de 11, ce qui termine ce cas.

Si n se termine par 90, alors $n+10$ ne se termine pas par 90 et on peut appliquer le raisonnement précédemment en remplaçant n par $n+10$.

En analysant la preuve précédente, il est facile de trouver un contre-exemple lorsqu'il est question de 38 entiers. Par exemple, on peut prendre les entiers compris entre 999 981 et 1 000 018.

<u>*Solution de l'exercice 39*</u> : Soient a un entier impair et b un entier pair tels que $b < a$. Notons u et v les racines de $x^2 - aX - b = 0$, avec $v < u$. On vérifie facilement que $u > 1$ et $-1 < v < 0$.

Pour $n > 0$ entier, on note $S_n = u^n + v^n$. Alors $S_1 = a$, $S_2 = a^2 + 2b$ et $S_{n+2} = aS_{n+1} + bS_n$. Puis, par récurrence on a S_n impair pour tout n. Or $u^n = S_n - v^n$ donc :

– si n est impair, on a $S_n < u^n < S_n + 1$ et donc $[u^n] = S_n$ est impair.

– si n est pair, on a $S_n - 1 < u^n < S_n$ et donc $[u^n] = S_n - 1$ est pair.

Le nombre u répond ainsi au problème.

Remarque. Si on veut une valeur particulière, on peut choisir $a = 3$ et $b = 2$, ce qui fournit $u = \frac{3+\sqrt{17}}{2}$.

<u>*Solution de l'exercice 40*</u> : On utilise ici le fait que :

$$(3n + 1)(3m + 1) = 3(3mn + m + n) + 1$$

ce qui incite à poser $n' = 3n + 1$ et $m' = 3m + 1$. Ce changement de variable effectué, l'équation fonctionnelle se réécrit :

$$f\left(\frac{m'n' - 1}{3}\right) = 4f\left(\frac{m' - 1}{3}\right) f\left(\frac{n' - 1}{3}\right) + f\left(\frac{m' - 1}{3}\right) + f\left(\frac{n' - 1}{3}\right)$$

Ainsi, si, pour n un entier de la forme $3k + 1$, on pose :

$$g(n) = f\left(\frac{n - 1}{3}\right)$$

on obtient l'équation fonctionnelle :

$$g(xy) = 4g(x)g(y) + g(x) + g(y)$$

ou encore en utilisant le même type de factorisation :

$$4g(xy) + 1 = (4g(x) + 1)(4g(y) + 1)$$

Posons finalement $h(x) = 4g(x) + 1$ pour obtenir $h(xy) = h(x)h(y)$. La fonction h n'est définie que sur l'ensemble $3\mathbf{N} + 1$ et prend ses valeurs dans l'ensemble $4\mathbf{N} + 1$ et elle réalise une bijection entre ces deux ensembles. D'autre part, si on arrive à construire une telle fonction h, on en déduira facilement une fonction f solution en posant :

$$f(n) = \frac{h(3n + 1) - 1}{4}$$

Le problème devient donc de construire h.

Notons pour cela $p_1, \ldots, p_n, \ldots$ la suite des nombres premiers congrus à 1 modulo 3. Notons également $p'_1, \ldots, p'_n, \ldots$ celle des nombres premiers congrus à 2 modulo 3, $q_1, \ldots, q_n, \ldots$

celle des nombres premiers congrus à 1 modulo 4 et $q'_1, \ldots, q'_n, \ldots$ celle des nombres premiers congrus à 3 modulo 4. Ces suites sont toutes infinies, par exemple d'après le théorème de Dirichlet.

Soit n un élément de l'ensemble $3\mathbf{N}+1$. Sa décomposition en nombres premiers peut s'écrire :

$$n = p_1^{\alpha_1} \ldots p_d^{\alpha_d} {p'}_1^{\alpha'_1} \ldots {p'}_{d'}^{\alpha'_{d'}}$$

puisque tout nombre premier sauf 3 est, de façon exclusive, soit un p_i, soit un p'_i. Cependant, 3 ne peut apparaître dans la décomposition de n puisque n étant congru à 1 modulo 3, il n'est pas divisible par 3. D'autre part, comme $n \equiv 1 \pmod 3$, le nombre $\alpha'_1 + \ldots + \alpha'_d$ doit être pair. Définissons :

$$h(n) = q_1^{\alpha_1} \ldots q_d^{\alpha_d} {q'}_1^{\alpha'_1} \ldots {q'}_{d'}^{\alpha'_{d'}}$$

Comme la somme $\alpha'_1 + \ldots + \alpha'_d$ est paire, on a bien $h(n) \equiv 1 \pmod 4$

La fonction h ainsi définie vérifie immédiatement $h(xy) = h(x)h(y)$ pous tous entiers x et y congrus à 1 modulo 3. En outre, elle est bijective, car on peut reconstruire n à partir de $h(n)$ en effectuant le même procédé à l'envers. Fini !

Solution de l'exercice 41 : Soit $\alpha > 0$ fixé. Pour $j \geqslant 2$, on pose :

$$n_j = \left[\frac{\alpha j}{\log j}\right]$$

On a $\log n_j \sim \log j$. Par ailleurs :

$$p_{n_j} \sim n_j \log n_j \sim n_j \log j \sim \alpha j$$

Soit alors $m_j = \left[\frac{j}{\log j}\right]$. Comme précédemment $p_{m_j} \sim j$ et donc la suite de terme général $\frac{p_{n_j}}{p_{m_j}}$ est à valeurs dans l'ensemble considéré et a pour limite α.

Solution de l'exercice 42 : On cherche n sous la forme $3^d - 2^d$ car la factorisation :

$$3^{kd} - 2^{kd} = \left(3^d - 2^d\right)\left(3^{(k-1)d} + 3^{(k-2)d} \cdot 2 + \cdots + 2^{(k-1)d}\right)$$

assure que si d divise n, alors $3^d - 2^d$ divise $3^n - 2^n$. De plus si d est un entier composé, alors il en sera de même de $3^d - 2^d$ encore par la même remarque.

On est donc ramené à trouver une infinité d'entiers d divisant $n - 1 = 3^d - 2^d - 1$. En fait, les puissances de 2 conviennent. En effet, si $d = 2^t$, on a directement d divise 2^d. Il reste à voir que d divise $3^d - 1$.

On montre ce dernier fait par récurrence sur l'entier t. Pour $t = 1$, on a bien $d = 2$ divise $3^d - 1 = 2$. Supposons que ce soit vrai pour l'entier t et remarquons que :

$$3^{2^{t+1}} - 1 = \left(3^{2^t} - 1\right)\left(3^{2^t} + 1\right)$$

Le premier facteur est divisible par 2^t par hypothèse de récurrence et le second est pair à l'évidence. Le produit est donc divisible par 2^{t+1}.

Finalement, on a démontré que tous les entiers n de la forme $3^{2^t} - 2^{2^t}$ sont composés pour $t \geqslant 1$ et conviennent, ce qui en fait indéniablement une infinité.

Remarque. En fait, tout nombre premier $n \geqslant 5$ convient également. C'est une conséquence directe du petit théorème de Fermat (voir 3.5). De façon plus générale, tous les nombres de Carmichael (voir 3.5) sont également solutions et on peut prouver qu'il en existe une infinité. Cependant cette dernière preuve est bien plus difficile que celle que l'on vient de donner pour résoudre l'exercice.

Solution de l'exercice 43 : Avant de commencer, définissons $\varphi(x) = \log_2 x = \frac{\log x}{\log 2}$ pour tout réel strictement positif x. Posons également $\varphi_k = \varphi \circ \cdots \circ \varphi$ (k fois) partout où c'est défini.

Construisons par récurrence des réels $x^{(k)}$ tels que la suite $\left(x_n^{(k)}\right)$ définie comme dans l'énoncé soit telle que $x_k^{(k)}$ soit un entier et un nombre premier et $\left[x_n^{(k)}\right] = \left[x_n^{(k-1)}\right]$ pour tout $k < n$. Il est évident de construire $x^{(0)}$, par exemple prenons $x^{(0)} = 2$.

Faisons l'hérédité. D'après le postulat de Bertrand, il existe au moins un nombre premier p compris strictement entre $2^{x_k^{(k)}}$ et $2^{x_k^{(k)}+1}$. Posons finalement $x^{(k+1)} = \varphi_{k+1}(p)$ (dont on vérifie facilement qu'il est bien défini). Directement, $x_{k+1}^{(k+1)} = p$ qui est par construction un nombre premier. D'autre part $2^{x_k^{(k)}} < p < 2^{x_k^{(k)}+1}$ et donc, en appliquant φ_1, on arrive à :

$$x_k^{(k)} < \varphi_1(p) < x_k^{(k)} + 1$$

et donc $[\varphi_1(p)] = x_k^{(k)}$ ou encore $\left[x_k^{(k+1)}\right] = x_k^{(k)}$. De même soit $2 \leqslant m \leqslant k$ un entier. En appliquant φ_m, on obtient :

$$\varphi_{m-1}\left(x_k^{(k)}\right) < \varphi_m(p) < \varphi_{m-1}\left(x_k^{(k)} + 1\right)$$

D'autre part, on constate qu'il ne peut pas y avoir d'entier entre les deux membres extrêmes de la précédente inégalité, car sinon il y aurait une puissance de 2 comprise strictement entre deux entiers consécutifs. On en déduit que :

$$[\varphi_m(p)] = \left[\varphi_{m-1}\left(x_k^{(k)}\right)\right]$$

ou encore :

$$\left[x_{k+1-m}^{(k)+1}\right] = \left[x_{k-m+1}^{(k)}\right]$$

ce qui achève la récurrence sauvagement.

Pour conclure, après avoir remarqué que la suite $\left(x^{(k)}\right)$ est décroissante, on note x sa limite. On laisse au lecteur le soin de rédiger l'argument de continuité montrant que x convient.

Solution de l'exercice 44 : Oui, c'est possible. Remarquons pour cela que la distance entre deux points A et B sur le cercle unité de centre O est donné par :

$$2\left|\sin\left(\frac{\widehat{AOB}}{2}\right)\right|$$

D'autre part, on remarque que si $\tan\theta$ est rationnel, alors il en est de même de $\sin(2\theta)$ en vertu de la formule :

$$\sin(2\theta) = \frac{2\tan\theta}{1 + \tan^2\theta}$$

Finalement, si $\tan\alpha$ et $\tan\beta$ sont rationnels, il en est de même de $\tan(\alpha+\beta)$ pourvu qu'il soit défini, à cause cette fois-ci de la formule :

$$\tan(\alpha+\beta) = \frac{\tan\alpha + \tan\beta}{1 - \tan\alpha\tan\beta}$$

Considérons donc θ un angle incommensurable avec π et dont la tangente est rationnelle[8]. Plaçons A_1 sur le cercle unité puis les points A_i $(2 \leqslant i \leqslant 1975)$ tels que l'angle $\widehat{A_1OA_i}$ vaille $4(i-1)\theta$. Comme θ est incommensurable avec π, les points A_i sont deux à deux distincts. En outre, la distance A_iA_j est donnée par la formule :

$$2\left|\sin\left(\frac{\widehat{A_iOA_j}}{2}\right)\right| = 2\left|\sin\left(2(i-j)\theta\right)\right|$$

qui est un nombre rationnel, en application des premières remarques.

<u>*Solution de l'exercice 45*</u> : Fixons k. On cherche à prouver qu'il existe une infinité d'entiers m tels que $f(m) = m-k$. On demande donc que $\sigma(m-k) \leqslant m$ et $\sigma(s) > m$ pour tout $s > m-k$.

Déjà si $s \geqslant m$, comme 1 et s sont diviseurs de s, on aura $\sigma(s) \geqslant s+1 \geqslant m+1 > m$. D'autre part, si s est composé, il admet un diviseur strict supérieur à $\sqrt{s}$ et donc $\sigma(s) \geqslant s + \sqrt{s}$.

L'idée est donc de choisir m tel que $m-k$ soit premier et tous les entiers compris entre $m-k+1$ et m soient composés avec $m \geqslant k^2+k-1$. En effet, on aura alors $\sigma(m-k) = m-k+1 \leqslant m$. Si s est compris entre $m-k+1$ et $m-1$, on aura :

$$\sigma(s) \geqslant s + \sqrt{s} \geqslant m-k+1+\sqrt{m-k+1} > m$$

Finalement si $s \geqslant m$, on aura forcément $\sigma(s) > m$.

Soit $p > k^2$ un nombre premier et soit $N = p(k+1)!+1$. Le nombre $N+1$ est pair, le nombre $N+2$ est multiple de 3, et de même pour tout i compris entre 1 et k, le nombre $N+i$ est multiple de $i+1$ et donc composé. Soit m_1-k le plus grand nombre premier inférieur à N. Ce nombre est supérieur à p et donc à k^2. Les nombres compris entre m_1-k+1 et m_1-1 sont tous composés et d'après ce qui a été vu précédemment m_1 vérifie bien $m_1 - f(m_1) = k$.

On recommence alors la même construction en partant de p un nombre premier supérieur à m_1. On trouve ainsi une nouvelle solution $m_2 > m_1$. Ainsi de suite, on construit une suite strictement croissante de solutions, ce qui prouve qu'il en existe une infinité.

<u>*Solution de l'exercice 46*</u> : La solution est $243 = 3^5$.

Définissons pour cela $S_n = \{3,\ldots,n\}$ et montrons dans un premier temps que S_{243} possède la propriété. En effet, soit X, Y une partition de S_{243}. On peut supposer que $3 \in X$. Si $9 \in X$, c'est gagné. On peut donc supposer que $9 \in Y$. Si $81 \in Y$, c'est gagné, on peut donc supposer que $81 \in X$. Si $27 \in X$, comme $3 \times 27 = 81$, c'est gagné, on peut donc supposer que $27 \in Y$. Enfin $243 = 3 \times 81 = 9 \times 27$, et on gagne dans chacun des cas.

[8] On peut montrer que l'angle $\arctan\left(\frac{4}{3}\right)$ convient, la preuve étant laissée au lecteur qui pourra judicieusement prouver que le nombre complexe $\left(\frac{3+4i}{5}\right)^n$ ne vaut jamais 1.

Pour pouvoir conclure, il suffit de montrer que S_{242} ne possède pas la propriété, c'est-à-dire d'exhiber une partition X, Y adéquate (pour $n < 242$, il suffira de prendre la partition $S_n \cap X$, $S_n \cap Y$). Pour cela nous allons définir l'ensemble P des nombres S-premiers :

$$P = \{4, 8, p, 2p \text{ où } p \text{ est un nombre premier } \geq 3\} \cap S_{242}$$

Les nombres S-premiers sont en fait les nombres qui ne sont pas le produit de nombres de S_{242}.

Comme le plus petit nombre S-premier de S_{242} est 3, chacun des nombres de S_{242} peut s'écrire comme produit d'au plus 4 nombres S-premiers d'au moins une façon (la décomposition en produit de nombres S-premiers n'est pas unique).

On note X la réunion des nombres S-premiers et des nombres de S_{242} qui peuvent s'écrire comme produit de 4 nombres S-premiers exactement, $Y = S_{242} \setminus X$.

Un nombre de Y possède au moins 2 facteurs S-premiers, donc un produit de 2 nombres de Y en possède au moins 4 ; s'il en a plus il est trop grand (car $4^4 > 242$). L'ensemble Y ne possède donc pas de triplet problématique. Maintenant, un produit de 2 nombres de X sera $\leqslant 242$ seulement s'il s'agit d'un produit de 2 nombres S-premiers. En regardant 4, 8, p_1, $2p_2$, on s'aperçoit qu'un produit deux nombres S-premiers ne peut se factoriser en un produit de 4 nombres S-premiers. L'ensemble X ne contient pas de triplet problématique non plus.

Solution de l'exercice 47 : Intéressons nous à la première somme et notons-la A. En inversant les indices de sommation, on constate que :

$$A = \sum_{k=1}^{p-1} \left[\frac{(p-k)^3}{p}\right] = \sum_{k=1}^{p-1} \left(p^2 - 3kp + 3k^2 + \left[\frac{-k^3}{p}\right]\right)$$

Or si x n'est pas un entier, on a $[-x] + [x] = -1$ et donc, comme p est premier :

$$2A = \sum_{k=1}^{p-1} \left(p^2 - 3kp + 3k^2 - 1\right) = \left(p^2 - 1\right)(p-1) - 3p\frac{p(p-1)}{2} + 3\frac{p(p-1)(2p-1)}{6}$$

Après simplification, on trouve :

$$A = \frac{(p-1)(p-2)(p+1)}{4}$$

Appelons B la seconde somme. On remarque que les valeurs prises par le terme que l'on somme sont comprises entre 0 et $p-2$. Soit n un entier compris entre 0 et $p-2$. On a $\left[\sqrt[3]{kp}\right] = n$ (pour k compris entre 1 et $(p-1)(p-2)$ si, et seulement si (puisque $\sqrt[3]{kp}$ n'est pas un entier, p étant premier) $\sqrt[3]{kp} - 1 < n < \sqrt[3]{kp}$ et puis :

$$\frac{n^3}{p} < k < \frac{(n+1)^3}{p}$$

De plus on a :

$$\left[\frac{(n+1)^3}{p}\right] < (p-1)(p-2)$$

pour tout n compris entre 0 et $p-2$. En effet, il suffit de le vérifier pour $n = p-2$, ce qui revient à voir que :

$$\frac{(p+1)^3}{p} < (p-1)(p-2)+1$$

ce que l'on vérifie directement en développant.

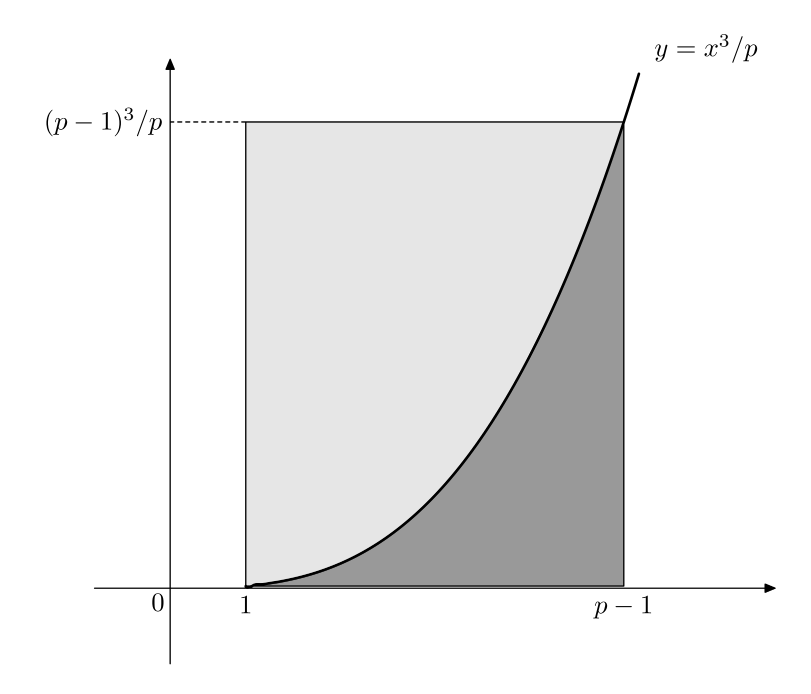
Ce qui précède assure que dans la somme B il y a exactement $\left[\frac{(n+1)^3}{p}\right] - \left[\frac{n^3}{p}\right]$ termes égaux à n. et donc :

$$B = \sum_{n=0}^{p-2} n \left(\left[\frac{(n+1)^3}{p}\right] - \left[\frac{n^3}{p}\right] \right) = (p-1)\left[\frac{(p-1)^3}{p}\right] - A$$

Un calcul analogue à celui qui a déjà été fait prouve que $\left[\frac{(p-1)^3}{p}\right] = (p-1)(p-2)$, et donc que :

$$B = \frac{(p-1)(p-2)(3p-5)}{4}$$

Remarque. La courbe représentée sur le dessin suivant est celle d'équation $y = \frac{x^3}{p}$. Dans ces conditions, on constate que A calcule le nombre de points à coordonnées entières dans la région en gris foncé, alors que B calcule le nombre de points à coordonnées entières dans la région gris clair :



Comme la courbe ne passe par aucun point à coordonnées entières, on en déduit que :

$$A + B = (p-1)\left[\frac{(p-1)^3}{p}\right] = (p-1)^2(p-2)$$

Solution de l'exercice 48 : **a)** Par récurrence, nous allons construire pour tout n une progression arithmétique de longueur n formée exclusivement de puissances parfaites. L'initialisation pour $n=1$ (ou $n=2$) est immédiate.

Supposons donc que l'on dispose d'un entier x et d'une raison r tels que, pour tout $k \in \{0,\ldots,n-1\}$, on ait $x+kr=a_k^{b_k}$ pour des entiers a_k et b_k avec $b_k>1$. Notons b le PPCM de tous les b_k, définissons $x'=(x+nr)^b x$ et $r'=(x+nr)^b r$. Soit $k \in \{0,\ldots,n-1\}$. Alors :

$$x'+kr'=(x+nr)^b(x+kr)=(x+nr)^b a_k^{b_k}$$

et comme par définition b_k divise b, le nombre $x'+k'r$ est bien une puissance parfaite. D'autre part $x'+nr'=(x+nr)^b x+n(x+nr)^b r=(x+nr)^{b+1}$ et est également une puissance parfaite. Cela conclut l'hérédité et la récurrence.

b) Montrons par l'absurde que ce n'est pas possible et donc qu'il existe un entier x et une raison r tels que $x+nr$ soit une puissance parfaite pour tout entier positif n. Soit $d=\text{PGCD}(x,r)$. Il existe des entiers y et s premiers entre eux tels que $x=dy$ et $r=ds$. Pour tout n, on a alors $x+nr=d(y+ns)$.

D'après le théorème de Dirichlet, il existe un nombre premier $p>d$ de la forme $y+ns$. Mais alors $v_p(x+nr)=1$ et $x+nr$ ne peut pas être une puissance parfaite. Contradiction.

Solution de l'exercice 49 : Supposons qu'il existe des rationnels x et y vérifiant l'équation. Soit p un nombre premier. Notons $\alpha=v_p(x)$ et $\beta=v_p(y)$ et supposons que l'un des deux nombres soient non nuls. La somme

$$x+y+\frac{1}{x}+\frac{1}{y}$$

doit être entière donc de valuation positive ou nulle, mais la valuation d'un des termes est strictement négative. La seule possibilité est d'avoir $\alpha=\pm\beta$, et ce pour tout p.

Ceci prouve qu'il existe des rationnels non nuls a et b tels que $x=ab$ et $y=\frac{a}{b}$. Écrivons $a=\frac{p}{q}$ et $b=\frac{s}{t}$ pour des entiers non nuls p, q, s et t tels que $\text{PGCD}(p,q)=\text{PGCD}(s,t)=1$. L'équation devient :

$$\frac{ps}{qt}+\frac{qt}{ps}+\frac{pt}{qs}+\frac{qs}{pt}=3n$$

soit après simplification :

$$\left(p^2+q^2\right)\left(s^2+t^2\right)=3npqst$$

Ainsi 3 divise l'un des deux facteurs du membre de gauche, par exemple p^2+q^2. On voit directement que cela implique que 3 divise p et 3 divise q, mais cela est impossible puisque p et q étaient supposés premiers entre eux.

Finalement, il n'y a bien aucune solution.

Solution de l'exercice 50 : On va prouver que si $n>0$, alors il y a exactement :

$$\frac{1}{2}\left(d\left(n^2\right)-2d(n)+1\right)$$

diviseurs positifs de n^2 qui sont inférieurs à n et ne divisent pas n.

En effet, si d est un diviseur de n^2, alors $d' = \frac{n^2}{d}$ en est aussi un et $d < n$ si et seulement si $d' > n$. Il y a donc exactement :

$$\frac{1}{2}\left(d\left(n^2\right) - 1\right)$$

diviseurs de n^2 qui sont strictement inférieur à n (et autant qui sont strictement supérieurs). Parmi ces diviseurs, il y a $d(n) - 1$ diviseurs de n qu'il faut éliminer pour notre dénombrement. La formule annoncée en découle.

Dans le cas particulier de $n = 2^{13} \times 3^{11} \times 5^7$, on calcule :

$$\begin{aligned} d\left(n^2\right) &= 27 \times 23 \times 15 = 9315 \\ d(n) &= 14 \times 12 \times 8 = 1344 \end{aligned}$$

Le nombre cherché est 3314.

Solution de l'exercice 51 : Notons $d = \text{PGCD}(a, b)$ et soient a' et b' des entiers tels que $a = da'$ et $b = db'$. L'équation devient :

$$c\left(a' + b'\right) = da'b'$$

d'où on déduit dans un premier temps que c divise $da'b'$. Comme a, b et c sont premiers entre eux dans leur ensemble, c est premier avec d et donc par le lemme de Gauss c divise $a'b'$.

D'autre part, on déduit également que a' divise $c(a' + b')$, mais comme a' est premier avec b' il est premier avec $a' + b'$ et donc a' divise c. De même, on trouve que b' divise c. Encore une fois parce que a' et b' sont premiers entre eux, cela implique $a'b'$ divise c.

Les entiers $a'b'$ et c sont positifs et se divisent mutuellement, donc $a'b' = c$ et $a' + b' = d$. En remultipliant par d, on trouve finalement $a + b = d^2$, ce qui conclut.

Solution de l'exercice 52 : **a)** Supposons que n soit de la forme $2^{k-1}\left(2^k - 1\right)$ avec $2^k - 1$ premier. On dispose de la décomposition en facteurs premiers de n et donc de l'expression de $\sigma(n)$:

$$\sigma(n) = \frac{2^k - 1}{2 - 1} \cdot \frac{\left(2^k - 1\right)^2 - 1}{\left(2^k - 1\right) - 1} = \left(2^k - 1\right)\left(2^k - 1 + 1\right) = 2n$$

Les nombres de cette forme sont donc bien parfaits et pairs (car la condition $2^k - 1$ premier implique $k \geqslant 2$).

Réciproquement, supposons que n soit un nombre parfait pair. Alors n s'écrit $n = 2^{k-1}A$ pour un certain entier $k \geqslant 2$ et un certain entier positif A impair. Par exemple, en décomposant A en facteurs premiers, on arrive à $\sigma(n) = \left(2^k - 1\right)\sigma(A)$ ce qui conduit, puisque n est supposé parfait, à :

$$2^k A = \left(2^k - 1\right)\sigma(A) \qquad (3)$$

Comme $2^k - 1$ est impair (et donc premier avec 2^k), le lemme de Gauss assure que $2^k - 1$ divise A et donc que l'on peut écrire $A = a\left(2^k - 1\right)$ pour un certain entier positif a. L'égalité (3) assure $\sigma(A) = A + a$. Puisque $k \geqslant 2$, les entiers A et a sont distincts et tous deux diviseurs de A. Ainsi, comme 1 est également diviseur de A, on doit avoir $a = 1$ pour que l'égalité

$\sigma(A) = A + a$ soit satisfaite. Cela implique $A = 2^k - 1$ et $\sigma(A) = A + 1$ et donc A premier. Finalement, n s'écrit bien sous la forme annoncée.

b) Supposons que n soit impair et ait au plus deux facteurs premiers. Alors on peut écrire $n = p^a q^b$ pour des nombres premiers impairs distincts $p < q$ et des entiers a et b positifs ou nuls. On a :

$$\frac{\sigma(n)}{n} = \frac{p^{a+1} - 1}{p^a (p-1)} \frac{q^{b+1} - 1}{q^b (q-1)} < \frac{p^{a+1}}{p^a (p-1)} \frac{q^{b+1}}{q^b (q-1)} = \frac{p}{p-1} \frac{q}{q-1}$$

D'autre part, on a forcément $p \geqslant 3$ et $q \geqslant 5$. Mais alors on obtient $\frac{\sigma(n)}{n} < \frac{3}{2} \times \frac{5}{4} < 2$ et donc n ne peut pas être parfait.

<u>*Solution de l'exercice 53*</u> : **a)** Notons $A = \text{PGCD}(a, a+5)$ et $B = \text{PGCD}(b, b+5)$. Ce sont des diviseurs de 5, ils sont donc égaux soit à 1, soit à 5.

Si $A = B$, en vertu de l'égalité $\text{PPCM}(x, y) \cdot \text{PGCD}(x, y) = xy$, l'équation devient $a(a+5) = b(b+5)$, ce qui implique $a = b$ puisque a et b sont positifs.

Par symétrie, on peut supposer $A = 1$ et $B = 5$ pour le cas restant. Dans ce cas, b est un multiple de 5, disons $b = 5b'$ et l'équation devient : $a(a+5) = b'(5b'+5) = 5b'(b'+1)$. On en déduit que 5 divise a, ce qui contredit $A = 1$.

b) La réponse est non. Supposons, par l'absurde qu'il existe a, b et c solutions. Notons $m = \text{PPCM}(a, b) = \text{PPCM}(a+c, b+c)$. Soit p un nombre premier diviseur commun de a et de b. Alors p divise m et donc p divise $a + c$ ou $b + c$. Dans un cas, comme dans l'autre, il divise c. En posant $a' = \frac{a}{p}$, $b' = \frac{b}{p}$ et $c' = \frac{c}{p}$, on obtient un nouveau triplet solution. En itérant le procédé, on peut supposer que a et b sont premiers entre eux dès le commencement.

Dans ces conditions, $m = ab$. Soit p un diviseur premier de $a + c$ et $b + c$. Alors p divise m, et donc il divise soit a, soit b. Il divise donc c et donc a et b. Cela est impossible car a et b sont premiers entre eux. Du coup, $a + c$ et $b + c$ sont également premiers entre eux et l'équation devient :

$$ab = (a+c)(b+c)$$

qui n'a manifestement pas de solution en entiers strictement positifs.

<u>*Solution de l'exercice 54*</u> : Soit p un nombre premier fixé, et α, β, γ les valuations p-adiques de a, b et c. On veut montrer que $\alpha + \beta + \gamma$ est un multiple de 3.

Pour cela, remarquons que :

$$v_p\left(\frac{a}{b} + \frac{b}{c} + \frac{c}{a}\right) \geqslant 0 \qquad (4)$$

et que l'on a la relation :

$$(\alpha - \beta) + (\beta - \gamma) + (\gamma - \alpha) = 0$$

Il en résulte que l'un au moins des trois entiers $\alpha - \beta$, $\beta - \gamma$, $\gamma - \alpha$ est négatif. Si aucun n'est strictement négatif, c'est que $\alpha = \beta = \gamma$ et $\alpha + \beta + \gamma$ est bien muliple de 3. Sinon, pour que (4) soit satisfaite, le minimum des trois valeurs doit être atteint au moins deux fois. Par exemple, on a $\alpha - \beta = \beta - \gamma$, ce qui assure que $\alpha + \beta + \gamma = 3\beta$ est encore multiple de 3.

Solution de l'exercice 55 : Montrons dans un premier temps qu'il existe des entiers x, y, z et t tels que $a = xy$, $b = zt$, $c = xz$ et $d = yt$. Définissons $x = \text{PGCD}(a, c)$, $y = \frac{a}{x}$, $z = \frac{c}{x}$ et $t = \frac{b}{z} = \frac{d}{y}$ comme on le vérifie immédiatement. Les quatre égalités voulues sont immédiates, et les nombres x, y et z sont manifestement des entiers. Le seul point qui n'est pas immédiat est de prouver que t est entier. Pour cela, considérons p un nombre premier. On a :

$$\begin{aligned} v_p(t) &= v_p(b) - v_p(z) = v_p(b) - v_p(c) + \min(v_p(a), v_p(c)) \\ &= v_p(d) - v_p(y) = v_p(d) - v_p(a) + \min(v_p(a), v_p(c)) \end{aligned}$$

Or $\min(v_p(a), v_p(c))$ vaut soit $v_p(a)$ et alors la première ligne prouve que $v_p(t) \geqslant 0$, soit $v_p(c)$ et c'est alors la deuxième ligne qui permet de conclure.

Forts de cette remarque, nous pouvons terminer l'exercice. On écrit simplement pour cela :

$$a^k + b^k + c^k + d^k = x^k y^k + z^k t^k + x^k z^k + y^k t^k = \left(x^k + t^k\right)\left(z^k + y^k\right)$$

et les deux facteurs précédents sont supérieurs ou égaux à 2.

Solution de l'exercice 56 : Supposons que le couple (m, n) soit solution. Alors le quotient $\frac{n^3+1}{mn-1}$ est entier, et donc il en est de même de :

$$\begin{aligned} m^3 \frac{n^3+1}{mn-1} &= \frac{(mn)^3 - 1}{mn-1} + \frac{m^3+1}{mn-1} \\ &= (mn)^2 + (mn) + 1 + \frac{m^3+1}{mn-1} \end{aligned}$$

On en déduit que (n, m) est également solution. Les rôles des deux variables sont donc symétriques et on peut ne chercher que les solutions pour lesquelles $m \geqslant n$.

Soit $K = \frac{n^3+1}{mn-1} \geqslant 1$. On a $n^3 + 1 = K(mn - 1)$ et donc n divise $K + 1$, puis $K = nx - 1$ pour un certain entier $x \geqslant 1$. Mais alors pour $n > 1$:

$$nx - 1 = K \leqslant \frac{n^3+1}{n^2-1} = n + \frac{1}{n-1}$$

Si de plus $n \geqslant 3$, il vient $n(x-1) < 2$ et donc $n(x-1) = 0$ (puisque c'est un multiple de n) puis $x = 1$. L'équation devient :

$$n - 1 = \frac{n^3+1}{mn-1}$$

d'où :

$$m = n + 1 + \frac{2}{n-1}$$

ce qui implique que $n - 1$ divise 2. Comme $n \geqslant 3$, la seule possibilité est $n - 1 = 2$, soit $n = 3$. Dans ce cas, $m = 5$ donne une solution.

Reste à regarder les cas $n = 1$ et $n = 2$. Pour $n = 1$, on doit avoir $m - 1$ divise 2 et donc $m = 2$ ou $m = 3$. Pour $n = 2$, il vient $2m - 1$ divise 9, puis $m = 2$ et $m = 5$ (car on suppose toujours $m \geqslant n = 2$).

Finalement, les solutions sont $(2, 1)$, $(3, 1)$, $(2, 2)$, $(5, 2)$, $(5, 3)$, $(1, 2)$, $(1, 3)$, $(2, 5)$ et $(3, 5)$.

Solution de l'exercice 57 : Soit r un nombre rationnel compris strictement entre $\frac{1}{2}$ et 2. Posons $r = \frac{m}{n}$. On remarque alors que $a = 2m - n$, $b = m + n$, $c = 2n - m$ et $d = m + n$ sont des entiers strictement positifs qui conviennent.

Pour le cas général, quitte à considérer l'inverse, on peut supposer $r \geqslant 1$. Il existe alors $n \geqslant 0$ tel que :

$$\frac{1}{2}\left(\frac{3}{2}\right)^{3n} < r \leqslant \frac{1}{2}\left(\frac{3}{2}\right)^{3n+3}$$

Ainsi $r\left(\frac{2}{3}\right)^{3n}$ est un rationnel strictement compris entre $\frac{1}{2}$ et 2. On utilise le résultat précédent :

$$r\left(\frac{2}{3}\right)^{3n} = \frac{a^3 + b^3}{c^3 + d^3}$$

pour certains entiers strictement positifs a, b, c et d. On en déduit :

$$r = \frac{(3^n a)^3 + (3^n b)^3}{(2^n c)^3 + (2^n d)^3}$$

ce qui assure la conclusion.

Solution de l'exercice 58 : Soit $r = p_1/q_1$ le rationnel que l'on veut écrire comme somme d'inverses d'entiers. On va voir que « l'algorithme glouton » consistant à soustraire à r la plus grande fraction $1/n$ possible fournit bien une solution au problème, et se termine en au plus p_1 étapes.

Plus précisément, construisons par récurrence les suites (p_k), (q_k) et (n_k) de la façon suivante : en supposant $p_k > 0$ et q_k construits, on note n_k le plus petit entier (nécessairement supérieur ou égal à 2) tel que $1/n_k \leqslant p_k/q_k$, et p_{k+1} et q_{k+1} sont le numérateur et le dénominateur de la fraction :

$$\frac{p_k}{q_k} - \frac{1}{n_k}$$

écrite sous forme irréductible. En particulier, p_{k+1} est un diviseur de $p_k n_k - q_k$. Or on a :

$$\frac{1}{n_k} \leqslant \frac{p_k}{q_k} < \frac{1}{n_k - 1}$$

ce qui donne $0 \leqslant p_k n_k - q_k < p_k$. Il en résulte que $0 \leqslant p_{k+1} < p_k$, et la suite (p_k) est donc strictement décroissante, et atteint en particulier la valeur 0 (car sinon l'algorithme continue).

Lorsque $p_{k+1} = 0$, la construction s'arrête, et l'on a :

$$r = \frac{1}{n_1} + \frac{1}{n_2} + \cdots + \frac{1}{n_k}$$

Reste à voir que les n_i sont tous distincts. En fait, $n_{i+1} > n_i$. En effet, si l'on avait $n_{i+1} \leqslant n_i$, on aurait $2/n_i \leqslant p_i/q_i$. Mais $1/(n_i - 1) \leqslant 2/n_i$, et donc $n_i - 1$ aurait dû être choisi à la place de n_i.

Remarque. La décomposition précédente n'est pas unique par exemple grâce à l'égalité :

$$\frac{1}{n} = \frac{1}{n+1} + \frac{1}{n\,(n+1)}$$

Solution de l'exercice 59 : Traitons d'abord le cas où $1 \in S$. Alors il existe un entier n tel que $p = n^2 + 1$. Cela implique $n > 2$ et n pair. On pose $a = p - (n-1)^2 = 2n$ et $b = p - 1 = n^2$ qui conviennent.

Maintenant si $1 \notin S$. Alors il existe $n > 2$ tel que :

$$n^2 + 1 < p < (n+1)^2 - 1 = n(n+2)$$

l'inégalité de droite étant stricte, car p est premier. On pose $a = p - n^2 \in S$. On a $a - n = p - n(n+1)$ qui est non nul puisque p est premier et strictement inférieur à n en valeur absolue. On pose $b = p - (a-n)^2 \in S$. On vérifie que $b = a(1 + 2n - a)$. On a $a < 2n$ et donc $1 + 2n - a > 1$ puis $a < b$. Le couple (a, b) convient.

Solution de l'exercice 60 : Pour $n \geqslant 0$, on considère le point A_n de coordonnées (n, n^2). La distance entre A_n et A_m est donnée par la formule :

$$\sqrt{(n-m)^2 + (n^2 - m^2)^2} = |n - m| \sqrt{(n+m)^2 + 1}$$

Si $n \neq m$, on a $|n - m| \neq 0$, et $n + m \geqslant 1$ ce qui implique que $(n+m)^2 + 1$ ne peut pas être un carré. La racine carrée écrite précédemment n'est pas un entier, c'est donc forcément un nombre irrationnel : en effet, s'il existe $x \in \mathbf{Q}$ tel que $x^2 = n$ pour un certain entier n fixé, on a $2v_p(x) = v_p(n) \geqslant 0$ pour tout nombre premier p et donc x est entier.

Il reste à voir que si n, m et p sont trois entiers distincts, alors l'aire du triangle dont les sommets sont A_n, A_m et A_p est rationnelle et non nulle. L'aire d'un tel triangle se calcule *via* :

$$\begin{aligned} \frac{1}{2} \det\left(\overrightarrow{A_n A_m}, \overrightarrow{A_n A_p}\right) &= \frac{1}{2}\left[\left(m^2 - n^2\right)(p-n) - \left(p^2 - n^2\right)(p-n)\right] \\ &= \frac{1}{2}(m-n)(p-n)(m-p) \end{aligned}$$

qui est bien non nul et rationnel.

Solution de l'exercice 61 : Soit n un entier. Notons $m = [\sqrt[3]{n}]$. Dire que n est divisible par tous les entiers inférieurs à $\sqrt[3]{n}$ revient à dire que n est divisible par $\text{PPCM}(1, 2, \ldots, m)$.

Deux nombres consécutifs sont forcément premiers entre eux. Ainsi le $\text{PPCM}(m, m-1) = m(m-1)$ et $\text{PPCM}(m-2, m-3) = (m-2)(m-3)$. Un nombre premier $p \geqslant 5$ ne peut diviser chacun de ces deux produits. Il en est de même de 4 et de 9. Ainsi le PGCD de $m(m-1)$ et de $(m-2)(m-3)$ est un diviseur de 6. On en déduit que :

$$\text{PPCM}(m, m-1, m-2, m-3) = \text{PPCM}(m(m-1), (m-2)(m-3))$$

est un multiple de :

$$\frac{m(m-1)(m-2)(m-3)}{6}$$

Ainsi n doit également en être un, et on obtient une inégalité :

$$(m+1)^3 \geqslant n \geqslant \frac{m(m-1)(m-2)(m-3)}{6}$$

que l'on peut réécrire :

$$m \leqslant 6\left(1+\frac{2}{m-1}\right)\left(1+\frac{3}{m-2}\right)\left(1+\frac{4}{m-3}\right)$$

ce qui n'est plus vérifié pour $m \geqslant 13$, et ne nous laisse qu'un nombre fini de vérifications à faire.

En réalité m ne peut valoir 13 : on calcule $\text{PGCD}\,(1,\ldots,13) = 360\,360$ et donc une solution n doit être multiple de 360 360 inférieur à $14^3 = 2744$. C'est impossible. De même on élimine les valeurs de m comprises entre 8 et 12.

Pour $m = 7$, on trouve $\text{PPCM}\,(1,\ldots,7) = 420$ et il existe bien (au moins) un multiple de 420 inférieur à $8^3 = 512$. Le plus grand est 420, c'est la réponse au problème !

Remarque. On peut en réalité légèrement ruser sur la fin pour éviter quelques calculs... mais bon.

Solution de l'exercice 62 : Tout d'abord, il est clair que le quotient :

$$q = \frac{abc-1}{(a-1)(b-1)(c-1)}$$

ne peut valoir 1. Comme c'est un entier, il est au moins égal à 2.

Remarquons ensuite que pour tout réel $x \geqslant 5$, on a $x - 1 \geqslant \frac{x}{\sqrt[3]{2}}$. Ainsi pour $a \geqslant 5$, on a :

$$2(a-1)(b-1)(c-1) \geqslant abc > abc - 1$$

et donc $abc - 1$ ne peut être divisible par $(a-1)(b-1)(c-1)$. On a donc prouvé que $2 \leqslant a \leqslant 4$.

Supposons $q = 2$. Alors abc est impair et d'après ce qui précède, a qui doit être impair ne peut valoir que 3. L'équation se réécrit $4(b-1)(c-1) = 3bc - 1$, soit $bc + 5 = 4b + 4c$, qui se réecrit $(b-4)(c-4) = 11$ qui conduit directement à la solution $b - 4 = 1$, $c - 4 = 11$, soit $b = 5$ et $c = 15$.

Supposons maintenant $q \geqslant 3$. Si $a = 2$, il vient $q(bc - b - c + 1) = 2bc - 1$, soit $(q-2)bc + (q+1) = qb + qc$ qui se factorise en :

$$[(q-2)b - q][(q-2)c - q] = q + 2 \tag{5}$$

On a $b \geqslant 3$, et si $c \geqslant 4$, on a $(q-2)b - q \geqslant 2q - 6$ et $(q-2)c - q \geqslant 3q - 8$. Ainsi le produit $[(q-2)b - q][(q-2)c - q] \geqslant (2q-6)(3q-8)$ et ce dernier minorant est strictement supérieur à $q + 2$ dès que $q \geqslant 4$. Il ne reste plus que la possibilité $q = 3$. Dans ce cas, il vient $(b-3)(c-3) = 5$ qui conduit à $b = 4$ et $c = 8$.

Si $a = 3$, on a $2q(bc - b - c + 1) = 3bc - 1$, soit $(2q-3)bc + (2q+1) = 2qb + 2qc$. Comme $b \geqslant 4$, on a $(2q-3)bc \geqslant (8q-12)c \geqslant 4qc > 2qc + 2qb$, il n'y a pas de solution.

Si $a = 4$, on écrit $(3q-4)bc + (3q+1) = 3qb + 3qc$. Mais $b \geqslant 4$, et donc $(3q-4)bc \geqslant (12q-16)c > 6qc > 3qb + 3qc$, et il n'y a pas non plus de solution.

En conclusion, les seules solutions sont $a = 2$, $b = 4$, $c = 8$ et $a = 3$, $b = 5$, $c = 15$.

Solution de l'exercice 63 : Soit $A = M^2 + M$, et a, b, c, d quatre éléments de S tels que $ab = cd$. On pose $a = A + x$, $b = A + y$, $c = A + z$ et $d = A + t$ de sorte que x, y, z et t sont en valeur absolue inférieurs ou égaux à M. L'égalité imposée s'écrit alors :

$$(x + y)A + xy = (z + t)A + zt$$

Si l'on a $x + y = z + t$, il vient $xy = zt$ et donc les paires $\{x, y\}$ et $\{z, t\}$ sont égales, et c'est terminé. Sinon, on écrit :

$$2M^2 \geqslant |xy - zt| = |(x + y) - (z + t)| \cdot |A| > |(x + y) - (z + t)| \cdot M^2$$

ce qui impose que les sommes $x + y$ et $z + t$ diffèrent de 1 exactement, par exemple $x + y = z + t + 1$, et par suite $xy = zt - A$. Alors x et y sont racines du trinôme :

$$X^2 - (z + t + 1)X + (zt - A)$$

Ls racines sont :

$$\frac{z + t + 1 \pm \sqrt{\Delta}}{2}$$

avec :

$$\Delta = (z + t + 1)^2 - 4zt + 4A \geqslant 4A = (z - t + 1)^2 + 4d \geqslant 4M^2$$

En fait, il ne peut y avoir égalité car sinon $d = M$ et $z - t + 1 = 0$, ce qui implique $t = -M$ et $z = -M - 1$, ce qui est interdit. Ainsi $\Delta > 4M^2$.

Donc si $z + t + 1 \geqslant 0$, la racine correspondant à $+\Delta$ est strictement supérieure à M, et si $z + t + 1 \leqslant 0$, la racine correspondant à $-\Delta$ est strictement inférieure à $-M$. Dans tous les cas, on obtient que x ou y dépasse M en valeur absolue, ce qui est absurde. D'où le résultat.

Solution de l'exercice 64 : Soit r le plus grand entier naturel tel que $2^r \leqslant n$. Alors pour tout k compris entre 1 et n, $v_2(k) \leqslant r$ avec égalité si et seulement si $k = 2^r$. On en déduit que :

$$v_2(H_n) = v_2 \left(1 + \frac{1}{2} + \cdots + \frac{1}{n} \right) = -r$$

et donc H_n n'est pas entier si $r \geqslant 1$, ce qui se produit dès que $n \geqslant 2$.

L'entier $m \geqslant 1$ étant fixé, notons d'autre part $u_n = H_{m+n} - H_m$. Notons $a_n = v_2(u_n)$. Nous allons montrer par récurrence que l'on a :

$$a_n = - \max_{1 \leqslant k \leqslant n} v_2(m + k)$$

C'est vrai pour $a_1 = v_2 \left(\frac{1}{m+1} \right)$. Supposons alors le résultat au rang n. Soit $v = v_2(m+n+1)$.

Si $v \neq -a_n$, on a $a_{n+1} = \inf(a_n, -v)$ et le résultat s'ensuit. Sinon, cela signifierait qu'il existe un entier k compris entre $m + 1$ et $m + n$ et de valuation v. Mais alors 2^v divise k et $m + n + 1$, et donc $m + n + 1 \geqslant k + 2^v$. Mais $v_2(k + 2^v) \geqslant v + 1$ (car k est de la forme $2^v(2k' + 1)$), ce qui contredit le fait que $a_n = -v$.

Finalement, on a montré que la différence $H_{m+n} - H_m$ n'était entière que pour $m = 0$ et $n = 1$.

Solution de l'exercice 65 : On a $d - a > c - b$ d'où en élevant au carré $a^2 - 2ad + d^2 > c^2 - 2bc + b^2$. En ajoutant $4ad = 4bc$ des deux côtés de l'inégalité, on obtient $(a+d)^2 > (b+c)^2$, soit encore :

$$a + d \geqslant b + c + 1$$

Si $\sqrt{d} - \sqrt{a} < 1$, on obtiendrait :

$$a + d < 1 + 2\sqrt{ad} = 1 + 2\sqrt{bc} \leqslant 1 + b + c \leqslant a + d$$

ce qui est absurde. On a donc forcément $\sqrt{d} - \sqrt{a} = 1$. On a alors :

$$a + d = 1 + 2\sqrt{ad} = 1 + 2\sqrt{bc} \leqslant 1 + b + c \leqslant a + d$$

et donc toutes les inégalités précédentes sont des égalités. Ainsi $b = c$ et donc $ad = b^2$. Notons p un diviseur premier commun à a et à d. Forcément p divise b et p divise $a + d = 2b + 1$, ce qui est impossible. Ainsi a et d sont premiers entre eux. Comme leur produit est un carré, a est également un carré.

Solution de l'exercice 66 : Montrons dans un premier temps que $2abc - ab - bc - ca$ ne peut s'écrire sous la forme $xbc + yca + zab$. En effet supposons que ce soit le cas. On aurait alors :

$$(x+1)\,bc = 2abc - ab - ca - yca - zab$$

et donc comme a, b et c sont premiers entre eux deux à deux, a devrait diviser $x + 1$. Ce dernier nombre ne peut être nul, puisque x doit être positif et donc on devrait avoir l'inégalité $x \geqslant a - 1$. De même, on prouve $y \geqslant b - 1$ et $z \geqslant c - 1$, mais alors :

$$\begin{aligned} xbc + yca + zab &\geqslant (a-1)\,bc + (b-1)\,ac + (c-1)\,ab \\ &= 3abc - bc - ac - ab > 2abc - ab - bc - ca \end{aligned}$$

d'où la contradiction.

Il faut désormais montrer que tout nombre strictement supérieur à $2abc - ab - bc - ca$ peut s'écrire sous la forme voulue. Puisque c et ab sont premiers entre eux, on sait que tout nombre strictement supérieur à $abc - ab - c$, disons d, peut s'écrire sous la forme $tc + zab$, pour t et z des entiers positifs. Maintenant, le nombre $ab - a - b + 1 + t$ est strictement supérieur à $ab - a - b$ et donc en appliquant à nouveau le même résultat, on voit que l'on peut écrire :

$$ab - a - b + 1 + t = xb + ya$$

pour certains entiers x et y encore positifs. Calculons :

$$xbc + yac + zab = (abc - ac - bc + c) + (tc + zab) = abc - ac - bc + c + d$$

On a bien prouvé que tout nombre de la forme $abc - ac - bc + c + d$ pour $d > abc - ab - c$, c'est-à-dire tout nombre strictement supérieur à $abc - ab - bc + c + abc - ab - c = 2abc - ab - bc - ca$, s'écrit de la forme voulue.

Solution de l'exercice 67 : On raisonne par l'absurde et on suppose qu'il existe α, β et γ strictement positifs tels que $S(\alpha)$, $S(\beta)$ et $S(\gamma)$ forment une partition de $\mathbf{N}^\star$. Les réels α, β et γ sont strictement supérieurs à 1, car si $0 < x < 1$, on a $S(x) = \mathbf{N}$.

On peut supposer $1 \in S(\alpha)$ et donc $\alpha < 2$. Il existe alors un entier $m \geqslant 2$:

$$1 + \frac{1}{m} \leqslant \alpha < 1 + \frac{1}{m-1}$$

Alors $[n\alpha] = n$ pour tout $n \leqslant m-1$ et $[m\alpha] = m+1$. Ainsi m est le plus petit entier n'appartenant pas à $S(\alpha)$. De plus deux éléments consécutifs n'appartenant pas à $S(\alpha)$ diffèrent de m ou de $m+1$.

Sans perte de généralité, on peut supposer $m \in S(\beta)$, ce qui assure que $[\beta] = m$. Ainsi deux éléments consécutifs de $S(\beta)$ diffèrent d'au plus $m+1$. Soit $n = [\gamma]$. Il est élément de $S(\gamma)$ et la minimalité de m assure qu'il existe x et y deux éléments consécutifs de $S(\beta)$ tels que $x < n < y$. La différence $y - x$ ne peut excéder $m+1$. Mais les différences $n - x$ et $y - n$ sont au moins égales à m. Ceci constitue une contradiction.

<u>*Solution de l'exercice 68*</u> : Soit a^2 un élément de cet hypothétique ensemble infini X. Alors, pour tout autre élément x^2 de X, il existe un entier $y > 0$ tel que $a^2 + x^2 = y^2$, c.à.d. $(y-x)(y+x) = a^2$ ce qui implique $x = \frac{p-q}{2}$ pour p et q des diviseurs de a^2 (en l'occurrence $y-x$ et $y+x$). Bref, tout élément de X différent de a^2 s'écrit comme la demi-différence de deux diviseurs de a^2. Comme il n'y a qu'un nombre fini de tels diviseurs, il ne peut donc y avoir qu'un nombre fini de tels x. D'où la conclusion.

<u>*Solution de l'exercice 69*</u> : On remarque immédiatement que 1992 est un multiple de 83, en l'occurrence $1992 = 83 \times 24$. Posons $x = 10^{83}$. Le nombre dont on veut calculer la partie entière est :

$$\begin{aligned} \frac{x^{23}}{x+7} &= x^{23}\left(1 - \frac{7}{x} + \left(\frac{7}{x}\right)^2 - \cdots + \left(\frac{7}{x}\right)^{22} - \left(\frac{7}{x}\right)^{23} + \frac{\left(\frac{7}{x}\right)^{24}}{1 + \frac{7}{x}}\right) \\ &= x^{23} - 7x^{22} + 7^2x^{21} - \cdots - 7^{23} + \frac{7^{24}}{x+7} \end{aligned}$$

Le dernier terme est compris strictement entre 0 et 1, donc la partie entière cherchée est donnée par :

$$x^{23} - 7x^{22} + 7^2x^{21} - \cdots - 7^{23}$$

Tous les termes sont des multiples de 10 sauf le dernier. En posant la soustraction, on voit que le chiffre cherché est le complémentaire à 10 du chiffre des unités de 7^{23}.

Le dernier de 7 est 7, celui de 7^2 est 9, celui de 7^3 est 3, puis 1 puis à nouveau 7. Comme pour calculer le dernier chiffre d'un produit, on multiplie les derniers chiffres des facteurs, on voit que la suite des derniers chiffres des puissances de 7 est périodique de période 4. Ainsi 7^{23} se termine par 3 et la réponse à la question est 7.

<u>*Solution de l'exercice 70*</u> : Supposons, par l'absurde, qu'il y ait une solution. Tout d'abord a_k ne peut être pair. En effet, si c'était le cas, $v_2(a_k!) > v_2(a_i!)$ pour tout $i < k$ et donc :

$$-n = v_2\left(\frac{1}{a_1!} + \cdots + \frac{1}{a_k!}\right) = v_2\left(\frac{1}{a_k!}\right) = -v_2(a_k!)$$

D'autre part :

$$-n = v_5\left(\frac{1}{a_1!} + \cdots + \frac{1}{a_k!}\right) \geqslant v_5\left(\frac{1}{a_k!}\right) = -v_5(a_k!)$$

On en déduit que $v_5(a_k!) \geqslant v_2(a_k!)$, ce qui est impossible puisque $a_k \geqslant 2$. Ce raisonnement fonctionne encore pour a_k impair et $a_{k-1} < a_k - 1$, ainsi que dans le cas $k = 1$.

Donc a_k doit être impair et $a_{k-1} = a_k - 1$. En réduisant au même dénominateur, en l'occurrence $a_k!$, on trouve que $a_k! = c10^n$ où :

$$c = 1 + a_k + a_k(a_k - 1)\cdots(a_{k-2}+1) + \cdots + a_k(a_k-1)\cdots(a_1+1)$$

On remarque que a_k et c sont premiers entre eux. Or a_k divise $10^n c$ donc il divise 10^n. Comme il est impair, il existe α positif ou nul tel que $a_k = 5^\alpha$. On a $a_{k-1} = a_k - 1 = 5^\alpha - 1$ est un multiple de 4. Ainsi $v_2(c) = 1$. On en déduit que $v_2(a_k!) = v_2(c10^n) = 1 + n$. De même $v_5(a_k!) = n$. Ainsi :

$$v_2(a_k!) = 1 + v_5(a_k!)$$

ce qui est impossible pour $a_k \geqslant 4$. On sait que a_k est une puissance de 5, donc $a_k = 1$ qui est exclus par $n > 0$.

Solution de l'exercice 71 : Si la décomposition en facteurs premiers de n est :

$$n = p_1^{\alpha_1}\cdots p_d^{\alpha_d}$$

le quotient qui nous intéresse vaut :

$$\frac{d(n^2)}{d(n)} = \frac{2\alpha_1+1}{\alpha_1+1}\cdots\frac{2\alpha_d+1}{\alpha_d+1}$$

Il s'agit donc simplement de voir quels nombres entiers peuvent s'écrire de cette façon. On constate tout d'abord que le numérateur est forcément impair, il en est donc de même du quotient.

Réciproquement, nous allons prouver par récurrence que tout nombre impair peut être obtenu. Pour les premières valeurs, on a :

$$3 = \frac{5}{3}\times\frac{9}{5} \quad ; \quad 5 = \frac{5}{3}\times\frac{5}{3}\times\frac{9}{5}$$

Pour l'hérédité, notons m le nombre impair que l'on cherche à obtenir. Notons k la valuation 2-adique de $m+1$ et posons :

$$\begin{aligned} a_1 &= \frac{\left(2^k-1\right)m-1}{2} \\ a_2 &= \frac{\left(2^k-1\right)m-1}{4} \\ &\vdots \\ a_k &= \frac{\left(2^k-1\right)m-1}{2^k} \end{aligned}$$

Tous ces nombres sont des entiers, puisque $a_k+1 = \frac{2^k-1}{2^k}(m+1)$ l'est. De plus $\frac{a_k+1}{2^k-1} = \frac{m+1}{2^k} < m$. D'après la définition de k, $\frac{m+1}{2^k}$ est impair et il relève donc de l'hypothèse de récurrence et on conclut en remarquant :

$$m = \frac{2a_1+1}{a_1+1}\cdots\frac{2a_k+1}{a_k+1}\times\frac{a_k+1}{2^k-1}$$

Solution de l'exercice 72 : L'astuce est d'utiliser judicieusement la condition $ad = bc$, en écrivant :

$$(b-a)(b+a) = b^2 - a^2 = \left(b^2 + bc\right) - \left(a^2 + ad\right) = 2^m b - 2^k a$$

D'autre part, on a $k > m$ car $a + d > b + c$ puisque $a(a + d - b - c) = (a - b)(a - c) > 0$. Ainsi $(b - a)(b + a)$ est multiple de 2^m. Comme b est impair, $(b - a) + (b + a) = 2b$ n'est pas multiple de 4, et donc il est impossible que $b - a$ et $b + a$ soient tous les deux multiples de 4. On en déduit que l'un d'entre eux est divisible par 2^{m-1}. Mais :

$$0 < b - a < b < \frac{b+c}{2} = 2^{m-1}$$

c'est donc $(a + b)$ qui est un multiple de 2^{m-1}. On a une autre inégalité :

$$b + a < b + c = 2^m$$

et donc $b + a = 2^{m-1}$.

Si d est un diviseur commun de a et de b, d doit diviser $a + b$ et donc être une puissance de 2. Puisque a et b sont impairs, il vient $d = 1$, c'est-à-dire que a et b sont premiers entre eux. De même, on prouve que a et c sont premiers entre eux en remarquant que $c - a = (c + b) - (b + a) = 2^m - 2^{m-1} = 2^{m-1}$.

Finalement a divise bc et est premier avec b et c. Donc $a = 1$.

5.2 Exercices de « *Division euclidienne et conséquences* »

Solution de l'exercice 73 : Le nombre $\overline{1010\,1\ldots1\,0101}^b$ (avec $2n + 1$ chiffres 1 au milieu) ne possède que des 1 à part aux positions 1, 3, $2n + 5$ et $2n + 7$ (le chiffre de droite étant en position 0). Ainsi on a :

$$\overline{1010\,1\ldots1\,0101}^b = \frac{b^{2n+9} - 1}{b - 1} - b - b^3 - b^{2n+5} - b^{2n+7}$$

la première fraction correspondant à un nombre de $2n + 9$ chiffres ne contenant que des 1. De même, on obtient :

$$\overline{1100\,1\ldots1\,0011}^b = \frac{b^{2n+9} - 1}{b - 1} - b^2 - b^3 - b^{2n+5} - b^{2n+6}$$

Il suffit donc de montrer que le quotient suivant :

$$\frac{b^{2n+9} - 1 - (b-1)\left(b + b^3 + b^{2n+5} + b^{2n+7}\right)}{b^{2n+9} - 1 - (b-1)\left(b^2 + b^3 + b^{2n+5} + b^{2n+6}\right)}$$

ne dépend pas de n, et donc par exemple est égal à sa valeur pour $n = 0$, qui se simplifie (on n'est pas obligé de le voir, mais bon) :

$$\frac{b^9 - 1 - (b-1)\left(b + b^3 + b^5 + b^7\right)}{b^9 - 1 - (b-1)\left(b^2 + b^3 + b^5 + b^6\right)} = \frac{b^4 - b^3 + b^2 - b + 1}{b^4 - b^2 + 1}$$

Pour cela, on calcule les produits en croix et on vérifie (péniblement) qu'ils sont égaux.

Solution de l'exercice 74 : On raisonne comme pour la décomposition en base b.

On remarque que si n s'écrit sous la forme :

$$n = a_1 1! + a_2 2! + a_3 3! + \cdots + a_d d! + \cdots$$

avec $0 \leqslant a_i \leqslant i$, alors a_1 est forcément le reste de la division euclidienne de n par 2 puisque la somme $a_2 2! + a_3 3! + \cdots$ est un multiple de 2. On pose donc la division euclidienne de n par 2 et on écrit :

$$n = 2q_1 + a_1$$

pour des entiers q_1 et a_1 avec $0 \leqslant a_1 \leqslant 1$. Il s'agit maintenant d'écrire q_1 sous la forme :

$$q_1 = a_2 \frac{2!}{2} + a_3 \frac{3!}{2} + \cdots a_d \frac{d!}{2} + \cdots$$

et pour cela on considère la division euclidienne de q_1 par 3. On écrit :

$$q_1 = 3q_2 + a_2$$

pour des entiers q_2 et a_2 avec $0 \leqslant a_2 \leqslant 2$. On veut alors écrire q_2 sous la forme :

$$q_2 = a_3 \frac{2!}{3!} + a_4 \frac{4!}{3!} + \cdots a_d \frac{d!}{3!} + \cdots$$

et on considère donc la division euclidienne de q_2 par 4, obtenant ainsi q_3 et a_3.

La suite des q_i est une suite d'entiers positifs et si $q_i > 0$, alors $q_{i+1} < q_i$. Il existe donc un entier d tel que $q_d = 0$ et à ce moment on a l'égalité :

$$n = a_1 1! + a_2 2! + a_3 3! + \cdots + a_{d-1} (d-1)!$$

Pour l'unicité, on remarque en analysant la construction précédente, qu'à chaque étape, on n'avait qu'un seul choix pour a_i.

Solution de l'exercice 75 : Dans un premier temps, on a $a_n \geqslant 1 = F_1$. D'autre part, par les propriétés de la division euclidienne, la suite des a_i est strictement décroissante. Ainsi $a_{n-1} \geqslant 2 = F_2$ et le quotient de la division euclidienne de a_i par a_{i-1} est toujours au moins 1. De cela, on déduit l'inégalité :

$$a_{i+1} \leqslant a_{i-1} - a_i$$

Une récurrence immédiate permet alors de prouver que pour tout $i \in \{1, \ldots, n\}$, on a $a_{n-i} \geqslant F_{i+1}$. Pour $i = n-2$, on obtient l'inégalité de l'énoncé.

Remarque. Cette inégalité assure la rapidité de l'algorithme d'Euclide. En effet, on peut montrer que l'on a une expression de F_n sous la forme $F_n = \frac{\sqrt{5}}{5}(\varphi^n - \bar{\varphi}^n)$ où $\varphi = \frac{1+\sqrt{5}}{2}$ et $\bar{\varphi} = \frac{1-\sqrt{5}}{2}$. Ainsi, on obtient :

$$a_2 \geqslant F_{n-1} \geqslant \frac{\sqrt{5}}{5}(\varphi^n - 1)$$

Ainsi le nombre d'étapes dans l'algorithme d'Euclide est majorée par un nombre de l'ordre de $\log_\varphi(a_2)$.

Solution de l'exercice 76 : Les entiers 3 et 5 sont premiers entre eux et liés par la relation de Bézout $2 \times 3 - 5 = 1$. Fixons un entier c. D'après le cours, l'équation :

$$5a + 3b = 2 - 15c$$

admet des solutions pour tout c qui sont données par $a = 15c - 2 - 3n$ et $b = 4 - 30c + 5n$ pour n décrivant $\mathbf{Z}$.

L'ensemble des solutions est donc l'ensemble des triplets $(15m-2-3n, 4-30m+5n, m)$ pour m et n décrivant $\mathbf{Z}$.

Remarque. L'ensemble des triplets (a, b, c) précédemment déterminés correspondent aux points à coordonnées entières sur le plan d'équation $5a + 3b + 15c = 0$.

Solution de l'exercice 77 : On sait que si n est un entier et que si s_n désigne la somme des chiffres de n en base 2, alors :

$$v_2(n!) = n - s_n$$

Ici, par hypothèse, $v_2(n!) \geqslant n - 1$. La seule possibilité est d'avoir $s_n = 1$, ce qui impose à n d'être une puissance de 2.

Solution de l'exercice 78 : On choisit un nombre n formé simplement avec des 0 et des 1 et suffisamment espacés pour que l'élévation au carré ne fasse pas intervenir de retenues.

On peut prendre :

$$n = \sum_{i=1}^{1997} 10^{2^{2i}}$$

Alors déjà l'écriture décimale n ne contient que des 0 mis à part 1997 fois le chiffre 1. On a donc bien $s(n) = 1997$. D'autre part, on aura :

$$n^2 = \sum_{i=1}^{1997} 10^{2^{2i+1}} + \sum_{1 \leqslant i < j \leqslant 1997} 2 \cdot 10^{2^{2i}+2^{2j}}$$

Les exposants qui apparaissent sont deux à deux distincts, comme on le voit en regardant leur écriture en base 2 par exemple. Il s'ensuit que n^2 possède 1997 chiffres 1, $\frac{1997\times1996}{2}$ chiffres 2 et sinon que des 0. On en déduit que $s(n^2) = 1997^2$.

Solution de l'exercice 79 : On remarque que si l'entier k vérifie $1 \leqslant k \leqslant n$ et est premier avec n, alors il en est de même de l'entier $n - k$. Ainsi on peut regrouper les nombres premiers avec n et inférieurs à n deux à deux, sauf éventuellement si $k = n - k$.

Ce dernier cas équivaut à $k = \frac{n}{2}$. Déjà, il ne peut se produire que si n est pair. Mais si $n > 2$ est pair, les nombres $\frac{n}{2}$ et n ne sont pas premiers entre eux.

Tout cela prouve que $\varphi(n)$ est toujours pair pour $n > 2$.

Solution de l'exercice 80 : Le déplacement ii) fait penser à l'algorithme d'Euclide. On se doute alors que la condition nécessaire et suffisante doit porter sur le PGCD de x et de y.

Plus précisément, nous allons montrer que le point (x, y) est *atteignable* si, et seulement si x et y sont strictement positifs et PGCD (x, y) est une puissance de 2.

On remarque dans un premier temps que si le couple (a, b) est formé d'entiers strictement positifs tels que PGCD (a, b) est une puissance de 2 alors il en est de même des couples $(a, 2b)$, $(2a, b)$, $(a - b, a)$ si $a > b$ et $(a, b - a)$ si $b > a$. Cela implique la nécessité de la condition : toute case (x, y) pouvant être atteinte par un jeton est telle que x et y sont strictement positifs et PGCD (x, y) est une puissance de 2.

Il reste à prouver que toutes ces cases peuvent effectivement être atteintes. Nous montrons cela par récurrence : au rang n, notre hypothèse de récurrence stipule que tout couple (x, y) vérifiant la condition précédente et tel que $x + y \leqslant n$ peut être atteint par un jeton. On initialise notre récurrence à $n = 2$, auquel cas le seul couple (x, y) d'entiers strictement positifs tel que $x + y \leqslant 2$ est le couple $(1, 1)$ qui est bien atteignable.

Traitons l'hérédité. Donnons-nous donc un couple (x, y) d'entiers strictement positifs tels que PGCD (x, y) soit une puissance de 2, et supposons que $x + y \leqslant n + 1$. Si x est pair, l'hypothèse de récurrence s'applique pour le couple $(\frac{x}{2}, y)$ et la transformation i) permet de conclure. On raisonne de même si y est pair. Sinon c'est que x et y sont impairs et donc premiers entre eux. S'ils sont égaux à 1, il n'y a rien à faire. Sinon, ils sont forcément distincts. Supposons par exemple $x < y$. Dans ce cas, on regarde le couple $(x, \frac{x+y}{2})$ qui relève de l'hypothèse de récurrence comme on le vérifie directement. Il peut donc être atteint. Une transformation de type i) permet alors de passer au couple $(x, x+y)$ puis une transformation de type ii) au couple (x, y) ce qui conclut.

<u>*Solution de l'exercice 81*</u> : Supposons que ces 14 entiers existent. Parmi eux, il en existe un, disons k, qui n'est ni le premier, ni l'un des trois derniers, qui est un multiple de 10. Ainsi $k - 1$, k, $k + 1$, $k + 2$ et $k + 3$ sont tous les cinq prodigieux. Nous allons montrer que cela est impossible.

Comme k est un multiple de 10, on a directement $P(k + i) = iP(k)$ pour $0 < i < 10$. En particulier, $P(k + 1) = P(k)$ et ce nombre doit diviser $k+1$ puisque $k+1$ est prodigieux. Or k est également prodigieux, donc $P(k)$ divise k et finalement $P(k) = 1$. Ainsi $P(k + 3) = 3$ divise $k + 3$ et donc k est un multiple de 3.

Comme $P(k) = 1$, l'entier k ne s'écrit qu'avec des 0 et des 1 et le chiffres de ses unités est 0. Ainsi $k - 1$ ne termine par un 9 et $P(k - 1)$ est un multiple de 3, et donc il en est de même de $k - 1$. Mais cela est impossible puisque déjà k était un multiple de 3.

<u>*Solution de l'exercice 82*</u> : Nous allons montrer par récurrence qu'il existe des suites (a_n) et (b_n) telles que $u_n = 2^{a_n} + 2^{b_n}$ pour tout n et les nombres $a_{n+1} - a_n$ et $b_{n+1} - b_n$ sont soit 0, soit 1. Il est clair que cela suffira pour conclure.

Pour $n = 1$ et $n = 2$, il suffit de prendre $a_1 = b_1 = a_2 = 0$ et $b_2 = 1$. Passons à l'hérédité. Si $u_{n+1} = 2u_{n-1}$, il suffit de prendre $a_{n+1} = a_{n-1} + 1$ et $b_{n+1} = b_{n-1} + 1$. Sinon, on a :

$$u_{n+1} = 3u_n - 2u_{n-1} = 2^{a_n} + 2^{b_n} + 2^{a_n+1} + 2^{b_n+1} - 2^{a_{n-1}+1} - 2^{b_{n-1}+1}$$

Alors si $a_n = a_{n-1} + 1$, on pose $a_{n+1} = a_n + 1$ et sinon (c'est-à-dire si $a_{n-1} = a_n$), on pose $a_{n+1} = a_n$. On fait de même avec b_n et cela termine l'hérédité et l'exercice.

Solution de l'exercice 83 : Supposons que les nombres x, x^2 et x^n aient tous les trois la même partie décimale. Déjà, on ne peut pas avoir $0 < x < 1$, car sinon les trois nombres seraient dans l'intervalle $[0, 1[$ et par le fait devraient être égaux.

Supposons donc $x > 1$. Alors $x^n > x^2 > x$ et la condition nous dit que les deux nombres $x^2 - x$ et $x^n - x$ sont entiers. On peut donc écrire $x^2 = x + a$ pour un certain entier $a > 0$. En multipliant par x, on obtient successivement :

$$\begin{array}{rcl} x^3 & = & x^2 + ax = x\,(a+1) + a \\ x^4 & = & x^2\,(a+1) + ax = x\,(2a+1) + \big(a^2 + a\big) \\ & \vdots & \end{array}$$

Et finalement par récurrence, on obtient $x^k = u_k x + v_k$ pour des entiers $u_k > a$ et v_k. Pour $k = n$, on obtient $x^n = u_n x + v_k$ et donc :

$$x^n - x = (u_n - 1)\,x + v_k$$

ce qui assure que $(u_n - 1)\,x$ est entier et donc que x est rationnel.

Supposons que x ne soit pas entier. Alors il existerait p un nombre premier tel que $v_p(x) < 0$. Mais alors $v_p(x^2) = 2v_p(x) < v_p(x)$ et donc $v_p(x^2 - x) = v_p(x^2) < 0$, ce qui n'est pas possible puisque $x^2 - x$ est un entier. On en déduit que x est entier.

Solution de l'exercice 84 : On définit une suite (a_n) par récurrence de la façon suivante. On pose $a_0 = 1$ et $a_1 = 2$. Puis $a_{n+1} = 1a_n$ (on ajoute 1 à gauche de l'écriture décimale de a_n) si 2^{n+1} ne divise pas a_n, et $a_{n+1} = 2a_n$ dans le cas contraire.

Il est clair que l'écriture décimale de a_n n'utilise que des 1 et des 2. On montre alors par récurrence que a_n est un multiple de 2^n. L'initialisation est immédiate. Et si on suppose que $a_n = 0 \pmod{2^n}$ alors :

- si $a_n \neq 0 \pmod{2^{n+1}}$ alors $a_n = 2^n \cdot b_n$ avec b_n impair. D'où $a_{n+1} = 10^n + a_n = 2^n(5^n + b_n) = 0 \pmod{2^{n+1}}$;
- si $a_n = 0 \mod [2^{n+1}]$ alors $a_{n+1} = 2 \cdot 10^n + a_n = 0 \mod 2^{n+1}$.

Solution de l'exercice 85 : **a)** Les deux réponses sont « oui ». Les nombres $a^2 - b^2$ et $a - b$ sont entiers, donc leur quotient $a + b$ est rationnel. Par suite la somme $(a - b) + (a + b) = 2a$ est également rationnelle et donc a est rationnel. On en déduit directement que b est aussi rationnel.

Montrons désormais que a et b sont entiers. On raisonne par l'absurde en supposant qu'il existe un nombre premier p tel que $v_p(a) < 0$. Comme $a - b$ est entier, il existe un entier k tel que $a = b + k$ et on a alors :

$$a^n - b^n = (b + k)^n - b^n = nb^{n-1}k + \mathrm{C}_n^2 b^{n-2}k^2 + \mathrm{C}_n^3 b^{n-3}k^3 + \cdots + k^n$$

Choisissons à partir de maintenant n premier à p, suffisamment grand. Alors on a :

$$v_p(nb^{n-1}k) = (n-1)\,v_p(b) + v_p(k)$$

qui est strictement négatif. De plus pour tout i compris entre 2 et k, on a :

$$v_p(\mathrm{C}_n^i b^{n-i}k^i) - v_p(nb^{n-1}k) = v_p(\mathrm{C}_n^i) + (i-1)\,v_p(k) - (i-1)\,v_p(b)$$

Le deux premiers termes du membre de droite sont positifs ou nuls et le troisième est strictement positif. On en déduit l'inégalité :

$$v_p(\mathrm{C}_n^i b^{n-i} k^i) > v_p(nb^{n-1}k)$$

et donc :

$$v_p(a^n - b^n) = v_p(nb^{n-1}k) < 0$$

ce qui est contradictoire.

b) Oui. Prenons par exemple $a = -\sqrt{2}$ et $b = 2 + \sqrt{2}$. La somme $a + b = 2$ est bien rationnelle. D'autre part, on vérifie par récurrence qu'il existe pour tout n des entiers u_n et v_n tels que :

$$\left(1 + \sqrt{2}\right)^n = u_n + v_n\sqrt{2}$$

où $u_n > 1$ et $v_n > 0$ dès que $n \geqslant 2$. On a ainsi :

$$b^n = \left(\sqrt{2}\right)^n \left(u_n + v_n\sqrt{2}\right)$$

Si $n = 2k$ est un nombre pair (avec $k \geqslant 1$), on en déduit :

$$a^n + b^n = 2^k \left(1 + u_n + v_n\sqrt{2}\right)$$

qui est bien irrationnel puisque v_n est non nul.

Si $n = 2k + 1$ est un nombre impair (avec $k \geqslant 1$), on obtient :

$$a^n + b^n = 2^k\sqrt{2}\left(-1 + u_n + v_n\sqrt{2}\right) = 2^{k+1}v_n + 2^k\left(u_n - 1\right)\sqrt{2}$$

qui est encore irrationnel puisque $u_n > 1$ et donc $u_n - 1$ est non nul.

Remarque. La méthode précédente est agréable car elle ne nécessite que peu de calculs. Toutefois, si on ne la trouve pas, on peut développer l'expression de $a^n + b^n$ grâce à la formule du binôme de Newton et parvenir plus laborieusement à la même conclusion.

c) Non. Si l'un des deux nombres (disons a) est nul, alors :

$$b = \frac{a^3 + b^3}{a^2 + b^2}$$

est rationnel.

Sinon, on peut écrire :

$$\begin{aligned} a + b &= \frac{(a^3 + b^3)(a^2 + b^2) - (a^5 + b^5)}{a^2 b^2} \\ a^2 b^2 &= \frac{1}{2}(a^2 + b^2)^2 - \frac{1}{2}(a^4 + b^4) \end{aligned}$$

La deuxième égalité prouve que a^2b^2 est rationnel et alors la première prouve qu'il en est de même de $a + b$.

Solution de l'exercice 86 : Il faut bien entendu comprendre que comme la martienne a six doigts à chaque main, elle a appris à compter en base 12. Les nombres de la formule sont donc écrits en base 12 : de fait 13 correspond à 15, 22 à 26 et 19 à 21. La formule de la martienne devient alors, version humaine :

$$(5x+3)(3x-7) = 15x^2 - 26x - 21$$

qui est un développement parfaitement correct.

Solution de l'exercice 87 : Il s'agit de montrer que la suite de Kolakoski ne devient jamais périodique. Notons u_n le n-ième terme de cette suite. Raisonnons par l'absurde et suppose qu'il existe un entier N et une période t tels que $u_{n+t} = u_n$ pour tout $n \geqslant N$. Choisissons t minimal pour cette propriété. Toute période est alors un multiple de t.

Notons a (resp. b) le nombre d'indices i ($N \leqslant i < N+t$) pour lesquels $u_i = 1$ (resp. $u_i = 2$). On a bien sûr $a+b=t$. D'autre part, par définition de la suite $a+2b$ est également une période et donc un multiple de $t = a+b$. Mais si ni a ni b n'est nul, on a :

$$a+b < a+2b < 2(a+b)$$

et donc $a+2b$ ne peut être un multiple de $a+b$. D'autre part $a=0$ est absurde car cela signifierait qu'il n'y a que des 1 dans la suite à partir d'un certain rang. De même $b=0$ est absurde.

On a finalement obtenu une contradiction : la suite (u_n) n'est pas périodique à partir d'un certain rang et le nombre x est irrationnel.

Solution de l'exercice 88 : Soit a un entier compris entre 1 et $n-1$. On va montrer que a et $k+a$ (considéré modulo n) ont la même couleur. Si $k+a<n$, il faut montrer que a et $k+a$ ont la même couleur, mais c'est évident puisque $|(k+a)-k| = a$.

Si $k+a \geqslant n$, il faut montrer que a et $k+a-n$ ont la même couleur. Mais $k+a-n$ a la même couleur que $n-a$ d'après la condition (2). Et $n-a$ a la même couleur que a d'après la condition (1).

On a ainsi prouvé que a a la même couleur que (le reste de la division euclidienne par n de) $a+\alpha k$ pour tout entier α. Comme k et n sont premiers entre eux, d'après le théorème de Bézout, il existe des entiers α et β tels que $\alpha k = 1 + \beta n$, soit :

$$a + \alpha k = (a+1) + \beta n$$

Ainsi a a toujours la même couleur que $a+1$. Cela conclut.

Solution de l'exercice 89 : Posons $s_n = 5^n + 7^n$. On remarque que :

$$\begin{aligned} s_n &= s_m s_{n-m} - 5^m 7^m s_{n-2m} \quad \text{si } n \geqslant 2m \\ s_n &= s_m s_{n-m} - 5^m 7^m s_{2m-n} \quad \text{si } n < 2m \end{aligned}$$

Ainsi $\text{PGCD}(s_n, s_m) = \text{PGCD}(s_m, s_{n-2m})$. En effectuant l'algorithme d'Euclide, et en utilisant le fait que m en n sont premiers entre eux, on voit que :
- si m et n sont de même parité (donc impairs), $\text{PGCD}(s_m, s_n) = \text{PGCD}(s_1, s_1) = 12$
- si n et m sont de parité contraire, $\text{PGCD}(s_m, s_n) = \text{PGCD}(s_0, s_2) = 2$

Solution de l'exercice 90 : Si ce nombre était rationnel, son écriture décimale serait périodique à partir d'un certain rang. Notons N un entier tel que p_N tombe dans la partie périodique. Il en sera de même de tout nombre premier p_n avec $n \geqslant N$.

Notons r la période. Par exemple, d'après le postulat de Bertrand (avec la constante 10 remplaçant 2 – ce qui est moins fort), il existe un nombre premier de k chiffres pour tout k. En particulier, il existe un nombre premier p_n (avec $n \geqslant N$) dont le nombre de chiffres est un multiple de r, supérieur à $2r$. Ce nombre doit être une répétition d'une séquence de r chiffres et par le fait doit être divisible par $1 \dots 1$ (r fois). Ainsi, il n'est pas premier. C'est une contradiction.

Autre solution. Soit n un entier. D'après le théorème de Dirichlet, il existe une infinité de nombres premiers congrus à 1 modulo 10^{n+1}. Ces nombres premiers possèdent une suite de n zéros consécutifs dans leur écriture décimale. Ainsi, le réel dont il est question a des suites de zéros consécutifs arbitrairement longues dans sa partie décimale. Si ce nombre était rationnel, sa période serait uniquement composée de zéros... or il est bien connu que les nombres premiers ne sont pas constitués exclusivement de zéros.

Solution de l'exercice 91 : On rappelle que l'on dispose d'une formule :

$$1^2 + 2^2 + \cdots + n^2 = \frac{n\,(n+1)\,(2n+1)}{6}$$

de laquelle on déduit :

$$2^2 + \cdots + n^2 = \frac{(n-1)\,(2n^2+5n+6)}{6}$$

et la condition dit alors simplement que ce dernier quotient doit être une puissance d'un nombre premier p. Ainsi, à part un facteur 2 et un facteur 3, le nombre premier p doit être le seul qui intervient dans la décomposition en facteurs premiers du produit $(n-1)\,(2n^2+5n+6)$. Si $n \geqslant 8$, chacun des facteurs est strictement supérieur à 6 et donc *doit* faire intervenir le nombre premier p dans sa décomposition en facteurs premiers. Ce p doit donc aussi intervenir dans la décomposition en facteurs premiers de $\text{PGCD}\,(n-1, 2n^2+5n+6)$.

On peut calculer ce PGCD par l'algorithme d'Euclide. On commence par écrire :

$$2n^2 + 5n + 6 = (n-1)\,(2n+7) + 13$$

ce qui prouve que $\text{PGCD}\,(n-1, 2n^2+5n+6) = \text{PGCD}\,(n-1, 13)$. Puisque 13 est un nombre premier, forcément, $p = 13$ et l'équation devient :

$$(n-1)\left(2n^2+5n+6\right) = 6 \times 13^k$$

On sait (toujours sous l'hypothèse $n \geqslant 8$) que l'on doit avoir $v_{13}\,(n-1) \geqslant 1$. Supposons $v_{13}\,(n-1) \geqslant 2$ ou autrement dit que $n \equiv 1 \pmod{169}$. Alors on vérifie que $2n^2+5n+6 \equiv 13 \pmod{169}$ et donc que $v_{13}\,(2n^2+5n+6) = 1$. D'autre part, on a vu que $v_2\,(2n^2+5n+6) \leqslant 1$, $v_3\,(2n^2+5n+6) \leqslant 1$ et $v_\ell\,(2n^2+5n+6) = 0$ pour tout ℓ différent de 2, 3 et 13. On en déduit l'inégalité $2n^2+5n+6 \leqslant 2 \times 3 \times 13 = 78$, qui n'est jamais vérifiée pour $n \geqslant 8$.

On en déduit que $v_{13}\,(n-1) = 1$ et donc que $n-1$ ne peut valoir que 13, 13×2, 13×3 ou 13×6, ce qui ne laisse qu'un nombre fini de cas que l'on vérifie à la main.

Les solutions sont les entiers $n = 2$, $n = 3$, $n = 4$ et $n = 7$.

Solution de l'exercice 92 : En réalité, après une étude attentive des cartes, on constate que la première carte réunit exactement les nombres dont l'écriture en base 2 se termine par un 1 (c'est-à-dire les nombres impairs), que la deuxième carte réunit les nombres dont l'avant-dernière chiffre de l'écriture en base 2 est un 1, et ainsi de suite.

Ainsi lorsque le partenaire montre les cartes, il donne l'écriture en base 2 du nombre qu'il a choisi. Il ne reste plus qu'à faire la conversion vers la base 10. Cela peut se faire simplement de la façon suivante : on additionne tous les nombres écrits en haut à gauche des cartes montrées, la somme est le nombre choisi.

Solution de l'exercice 93 : Notons a, b et c trois éléments distincs de A. Il s'agit de montrer que l'on ne peut pas avoir $a + c = 2b$. Le nombre b ne s'écrit qu'à l'aide de 0 et de 1 en base 3, ainsi le nombre $2b$ n'utilise, lui, que des 0 et des 2.

Notons de plus que l'addition de a par c ne peut pas faire intervenir de retenus. Comme a et c sont distincts, il existe un rang n tel que le n-ième chiffre (en partant de la droite) de a et de c diffèrent. Ainsi l'un vaut 0 et l'autre 1, et la somme fait 1. Forcément, donc, dans la somme $a + c$ écrite en base 3 possède un 1 ; elle ne peut donc égaler $2b$.

Solution de l'exercice 94 : Effectuons la division euclidienne de a par b : il existe q et r tels que $a = bq + r$ et $0 \leqslant r < b$. On a alors :

$$2^a + 1 = 2^{bq+r} + 1 = \left(2^{bq+r} - 2^r\right) + (2^r + 1) = 2^r \left(2^{bq} - 1\right) + (2^r + 1)$$

Or la factorisation :

$$2^{bq} - 1 = \left(2^b - 1\right)\left(2^{b(q-1)} + 2^{b(q-2)} + \cdots + 1\right)$$

montre que $2^{bq} - 1$ est un multiple de $2^b - 1$. Ainsi, pour notre situation, il faut que $2^r + 1$ soit un multiple de $2^b - 1$, et donc en particulier $2^r + 1 \geqslant 2^b - 1$. De plus $r < b$, donc en regroupant on obtient $0 < 2^b - 2^r \leqslant 2$, qui n'a pas de solution puisque l'on a supposé $b > 2$.

Solution de l'exercice 95 : Pour tout $k \geqslant 0$, on note P_k le polynôme $P \circ \cdots \circ P$ obtenu en composant P k fois avec lui-même. En particulier, pour tout i, $a_{i+k} = P_k(a_i)$. On pose de plus $d = \text{PGCD}(a_m, a_n)$, et si par exemple $m \geqslant n$, on note $m = n + k$. Il vient ainsi, avec des notations évidentes :

$$a_m = P_k(a_n) = a_n \left(\sum_{r \geqslant 1} \alpha_r a_n^{r-1}\right) + P_k(0)$$

Il en résulte que d divise $P_k(0) = P_k(a_0) = a_k = a_{m-n}$. Par une récurrence du type de l'algorithme d'Euclide, il en résulte aussitôt que d divise $a_{\text{PGCD}(m,n)}$.

Il s'agit alors réciproquement de voir que $a_{\text{PGCD}(m,n)}$ divise a_m, ou plus généralement que pour tout i et tout $r \geqslant 1$, a_i divise a_{ri}. Mais c'est clair par récurrence : a_i se divise lui-même, et si a_i divise a_{ri}, alors le calcul précédent montre qu'il divise aussi $P_i(a_{ri}) = a_{(r+1)i}$ puisque c'est le coefficient constant de P_i.

On a donc bien montré que pour tous m, n, on a :

$$\text{PGCD}(a_m, a_n) = a_{\text{PGCD}(m,n)}$$

Solution de l'exercice 96 : Notons $z = \frac{a}{b} = x + iy$. Notons x' (resp. y') un entier tel que $|x - x'| \leqslant \frac{1}{2}$ (resp. $|y - y'| \leqslant \frac{1}{2}$). Posons finalement $q = x' + iy'$ et $r = a - bq$. On a :

$$\left|\frac{r}{b}\right| = |(x - x') + i(y - y')| = \sqrt{(x - x')^2 + (y - y')^2} \leqslant \frac{\sqrt{2}}{2} < 1$$

Ainsi $|r| < |b|$ comme on le souhaite.

La décomposition n'est pas unique comme le montre l'exemple suivant :

$$1 = 0 \times 2 + 1 = 1 \times 2 - 1$$

Notons que ce contre-exemple est déjà valable dans $\mathbf{Z}$: la condition de positivité est donc essentielle à l'unicité et il est difficile d'en donner un équivalent convaincant sur $\mathbf{Z}[i]$.

Commentaire. Un ensemble de nombres sur lequel on dispose d'une telle division est un *anneau euclidien*. Comme dans l'exemple de $\mathbf{Z}$, cette propriété en implique de nombreuses autres bien utiles : existence de PGCD, existence et unicité de la décomposition en facteurs premiers...

Solution de l'exercice 97 : On remarque aisément que $1994 = 997 \times 2$ s'écrit 22 en base 996.

Supposons que 1993 soit brésilien. Dans ce cas, il existerait des entiers a, b et k avec $1 \leqslant a < b < 1992$ tels que :

$$1993 = a \cdot \frac{b^k - 1}{b - 1}$$

Or, 1993 est un nombre premier. Donc, forcément $a = 1$. En écrivant 1993 en base $2, \ldots, 6$, on voit que forcément $b \geqslant 7$. Ceci implique $k \leqslant 3$. D'autre part $k \geqslant 3$ car les hypothèses faites assurent que le nombre ne peut avoir un chiffre ou deux chiffres égaux à 1. Il ne reste plus qu'à résoudre :

$$1 + b + b^2 = 1993$$

et on vérifie que les solutions de cette équation ne sont pas entières.

Solution de l'exercice 98 : On va montrer que parmi les termes de la suite, on peut trouver une série de 1 aussi longue que l'on veut. Comme d'un autre côté, on va prouver que la suite n'est pas constante à partir d'un certain rang, cela permettra directement de conclure.

Prenons $n = 10^j$. Alors $n^k = 10^{jk}$ commence par 1, donc $x_n = 1$. Mais le nombre $\left[10^j \times \sqrt[k]{2}\right]^k < 2 \times 10^{jk}$ commence par un 1 également. De façon plus générale, pour tout i compris entre 10^j et $\left[10^j \times \sqrt[k]{2}\right]$, on a $x_i = 1$. Le nombre de i concernés par cette dernière propriété croît indéfiniment avec j, ce qui assure la première partie de la conclusion.

D'autre part, pour tout j, le nombre $\left(1 + \left[10^j \times \sqrt[k]{2}\right]\right)^k$ commence par un 2, ce qui suffit pour conclure.

Solution de l'exercice 99 : Le nombre de chiffres d'un entier n en base b est donné par :

$$1 + \left[\frac{\log n}{\log b}\right]$$

Ainsi, si l'on définit pour $n > 0$:

$$u_k = \left[\frac{\log 10^k}{\log 2}\right] = \left[\frac{\log 10}{\log 2}k\right]$$
$$v_k = \left[\frac{\log 10^k}{\log 5}\right] = \left[\frac{\log 10}{\log 5}k\right]$$

il s'agit de prouver que l'ensemble des valeurs prises par les suites u_k et v_k forment une partition de $\mathbf{N}^\star$. D'après le théorème de Beatty, il suffit pour cela de vérifier que $\frac{\log 10}{\log 2}$ et $\frac{\log 10}{\log 5}$ sont irrationnels et que :

$$\frac{\log 2}{\log 10} + \frac{\log 5}{\log 10} = 1$$

La deuxième condition est immédiate. Pour vérifier que le nombre $\frac{\log 10}{\log 2}$ est irrationnel, on suppose qu'il s'écrit $\frac{m}{n}$ pour certains entiers m et n strictement positifs, ce qui donne $10^m = 2^n$. C'est impossible.

Solution de l'exercice 100 : Notons $n = dd'$. La deuxième condition de l'énoncé devient $d^2d'+1$ divise $d^2(d'^2+1)$. Les nombres $d^2d'+1$ et d^2 sont premiers entre eux, donc le lemme de Gauss assure que $d^2d'+1$ divise d'^2+1.

On a $d'^2+1 = (d^2d'+1) + d'(d'-d^2)$ et donc $d^2d'+1$ doit divise $d'(d'-d^2)$ puis $d'-d^2$ en appliquant à nouveau le lemme de Gauss. On a :

$$\frac{d'-d^2}{d^2d'+1} = \frac{d'}{d^2d'+1} - \frac{d^2}{d^2d'+1}$$

et les deux termes du membre de droite sont compris strictement entre 0 et 1. Leur différence, qui doit être un entier, est donc forcément nulle. On en déduit que $d' = d^2$ puis $n = d^3$.

Réciproquement, on vérifie immédiatement que ces solutions conviennent.

Solution de l'exercice 101 : Soit $0 \leqslant x < n!$ un entier. Nous allons montrer qu'il existe des entiers a_i tels que :

$$x = a_1 n! + a_2\frac{n!}{2!} + a_3\frac{n!}{3!} + \cdots + a_n\frac{n!}{n!}$$

avec $0 \leqslant a_i < i$. Cela conclura car on vérifie directement que chacun de termes non nuls $a_i\frac{n!}{i!}$ est un diviseur de $n!$ et que si $i < j$ et si a_i et a_j sont non nuls alors $a_i\frac{n!}{i!} > a_j\frac{n!}{j!}$. Par ailleurs, il est facile de traiter le cas $x = n!$ à part.

Pour démontrer la propriété, on raisonne par récurrence sur n. On commence par poser la division euclidienne de x par n qui s'écrit $x = nq + a_n$ avec $0 \leqslant a_n < n$. Il s'agit alors d'écrire l'entier q sous la forme :

$$q = a_1(n-1)! + a_2\frac{(n-1)!}{2!} + a_3\frac{(n-1)!}{3!} + \cdots + a_{n-1}\frac{(n-1)!}{(n-1)!}$$

mais c'est exactement l'hypothèse de récurrence : il suffit de vérifier que $q < (n-1)!$ ce qui est immédiat.

Solution de l'exercice 102 : Si n est impair, alors 1 et 2 sont premiers avec n et donc il en est de même de tous les entiers strictement inférieurs à n. Donc n est premier.

Si $n = 4k$, alors $2k-1$ et $2k+1$ sont premiers avec n et inférieurs à n, et donc il en est de même de tous les entiers impairs inférieurs à n. Ainsi n est une puissance de 2.

Si $n = 4k+2$, alors $\text{PGCD}\,(2k+3, n) = \text{PGCD}\,(2k+3, 2k+1)$ car $2k+3$ est impair. Ce PGCD doit diviser 2 mais ne peut être pair, c'est donc 1. De même $2k+5$ est premier avec n. De plus comme $n > 6$, il est inférieur à n et le même argument que précédemment prouve que n ne peut-être une solution.

Solution de l'exercice 103 : Supposons que a_n soit pair et notons k sa valuation 2-adique. Le nombre $\frac{3}{2}a_n$ est alors entier et de valuation 2-adique $k-1$. On voit directement par récurrence que pour $i \leqslant k$, $v_2\,(a_{n+i}) = k - i$ et donc a_{n+k} est impair. Ceci démontre qu'il y a une infinité de termes impairs.

De même, si a_n est impair, on note k la valuation 2-adique de $a_n - 1$. Le nombre $\frac{3}{2}a_n$ n'est pas entier et donc sa partie entière vaut $a_{n+1} = \frac{3}{2}a_n - \frac{1}{2} = a_n + \frac{a_n - 1}{2}$. Ainsi :

$$a_{n+1} - 1 = \frac{3}{2}\,(a_n - 1)$$

et donc la valuation 2-adique de ce nombre est $k-1$. Comme ci-dessus, il vient $a_{n+k} - 1$ est impair et a_{n+k} est pair.

Remarque. Les propriétés précédentes se *voient* lorsque l'on écrit les nombres a_n en base 2.

Solution de l'exercice 104 : Clairement, les puissances de nombres premiers conviennent. Soit n une solution qui ne n'est pas une puissance de nombre premier. Soit p le plus petit diviseur premier de n. On pose $n = p^\alpha k$ où k est premier avec p. Notons que $k \geqslant 2$.

Puisque k est un diviseur de n, tout diviseur de k est aussi un diviseur de n. Les entiers p et k sont des diviseurs de n premiers entre eux, on doit donc avoir $p+k-1$ divise n. Si ℓ est un nombre premier divisant $p+k-1$, il doit diviser n. Si $\ell \neq p$, il divise en outre k et donc $p-1$, ce qui n'est pas possible. Ainsi p est le seul diviseur premier de $p+k-1$ et donc $p+k-1 = p^a$ pour un certain entier $a \geqslant 2$. Ainsi p^2 divise n.

Supposons k et $p+1$ premiers entre eux. Alors k et p^2-1 sont également premiers entre eux. En appliquant l'hypothèse p^2+k-1 divise n. Comme ci-dessus, on en déduit que $p^2+k-1 = p^b$ pour un certain entier b strictement supérieur à a. Dans ces conditions, il vient :

$$p^2 - p = p^b - p^a$$

et comme $b > a \geqslant 2$, on en déduit que p^2 divise p, ce qui est absurde.

Par suite, $d = \text{PGCD}\,(k, p+1) = \text{PGCD}\,(k, p^2-1) > 1$. Or, si d divise $p+1$ et k, il divise aussi n et la minimalité de p assure alors que $p = 2$ et $d = 3$ et que k est impair. De plus, on sait que $k+1 = 2^a$. Cette fois, on a $p^2+k-1 = k+3$ qui est divisible par 2, par 3, mais ni par 9 (puisque sinon k serait également divisible par 9 et donc 3 le serait aussi) ni par aucun autre nombre premier $q > 3$ qui divise n. Par suite $k+3 = 3 \cdot 2^b$, où $b \geqslant 1$. Ainsi, il vient $2 + 2^a = 3 \cdot 2^b$ et donc facilement $a = 2$ et $b = 1$, puis $k = 3$ et $n = 3 \cdot 2^\alpha$, avec $\alpha \geqslant 2$. Si $\alpha \geqslant 3$ alors $2^3 + 3 - 1 = 10$ doit diviser n, ce qui est absurde. Donc $\alpha = 2$ et $n = 12$ qui effectivement est bien une solution.

Finalement, les solutions sont les puissances de nombres premiers et $n = 12$.

Solution de l'exercice 105 : Appelons A, B et C les trois boîtes. Elles contiennent respectivement a, b et c jetons. Sans perte de généralité, on peut supposer que $1 \leqslant a \leqslant b \leqslant c$.

On pose $b = aq + r$ avec $0 \leqslant r < a$ et $q \geqslant 1$ la division euclidienne de b par a. Soit $q = m_0 + 2m_1 + \cdots + 2^k m_k$ l'écriture de q en base 2 (avec donc $m_k = 1$ et $m_i \in \{0, 1\}$ pour tout i).

Comme $c \geqslant b$, il y a au moins $2^k a$ jetons dans la boîte C. On double alors k fois de suite le nombre de jetons dans A par les transvasements suivants : à l'étape i, si $m_i = 1$ on prend les $2^i a$ jetons dans B, et si $m_i = 0$, on les prend dans C. Il y en aura bien suffisamment dans C car $2^k \geqslant 1 + 2 + \cdots + 2^{k-1}$.

À l'issue de ces opérations, on se retrouve avec $2^{k+1}a$ jetons dans A, r jetons dans B et le reste dans C. En particulier, la boîte qui contient le moins de jetons en contient strictement moins que a. En répétant la procédure précédente, on finira par obtenir une boîte vide.

Solution de l'exercice 106 : Commençons par exprimer les termes de la suite en fonction de x_0. On peut le faire à l'aide du développement en base 2.

On peut bien sûr supposer que $x_0 < 1$, et on écrit alors le développement en base 2 de x_0 sous la forme :

$$x_0 = 0, a_1 a_2 \ldots$$

Alors on a $2x_0 = a_1, a_2 a_3 \ldots$ Si $a_1 = 1$, il vient donc :

$$|1 - 2x_0| = 2x_0 - 1 = 0, a_2 a_3 \ldots$$

et si à l'inverse $a_1 = 0$, on a :

$$|1 - 2x_0| = 0, \bar{a_2}\bar{a_3} \ldots \quad \text{où l'on note } \bar{0} = 1 \text{ et } \bar{1} = 0$$

On obtient ainsi :

$$x_1 = 1 - |1 - 2x_0| = \begin{cases} 0, a_2 a_3 \ldots & \text{si } a_1 = 0 \\ 0, \bar{a_2}\bar{a_3} \ldots & \text{sinon} \end{cases}$$

Par une récurrence immédiate, on obtient le terme de rang n de la suite :

$$x_n = \begin{cases} 0, a_{n+1} a_{n+2} \ldots & \text{s'il y a un nombre pair de 1 parmi } a_1, \ldots, a_n \\ 0, \bar{a_{n+1}}\bar{a_{n+2}} \ldots & \text{sinon} \end{cases}$$

Cela étant, si x_0 est rationnel, son développement en base 2 est périodique à partir d'un certain rang N, de période k. Alors pour tout $n \geqslant N$, il y a nécessairement un nombre pair de 1 parmi les chiffres $a_{n+1}, \ldots, a_{n+2k}$ qui forment deux périodes consécutives, et bien sûr $a_{n+2k+\ell} = a_{n+\ell}$ pour tout ℓ. Il en résulte que $x_n = x_{n+2k}$ pour tout $n \geqslant N$, et donc (x_n) est périodique de période au plus $2k$ à partir du rang N.

Réciproquement, supposons (x_n) périodique à partir du rang N, et notons k une période. En comparant les chiffres de x_n et x_{N+k}, il vient (selon la parité du nombre de 1 parmi $a_{N+1}, \cdots, a_{N+k}$) ou bien $a_{n+k} = a_n$ pour tout $n \geqslant N + 1$, ou bien $a_{n+k} = \bar{a_n}$ pour tout $n \geqslant N + 1$. Dans tous les cas, $a_{n+2k} = a_n$ pour tout $n \geqslant N + 1$, et donc la suite des chiffres binaires de x_0 est périodique à partir du rang $N + 1$, ce qui entraîne que x_0 est rationnel.

Finalement, la suite (x_n) est périodique si et seulement si x_0 est rationnel.

Solution de l'exercice 107 : **a)** On raisonne par récurrence sur p. Pour $p = 1$, la formule dit simplement que $F_{n+1} = F_{n+1}$, ce qui est certainement vrai. Pour $p = 2$, la formule redonne

la relation de récurrence qui définit la suite de Fibonacci. Supposons donc la formule vraie aux rangs p et $p+1$, et prouvons-là pour le rang $p+2$. On calcule :

$$\begin{aligned} F_{n+p+2} &= F_{n+p+1} + F_{n+p} = F_p F_n + F_{n+1} F_{p+1} + F_{p-1} F_n + F_{n+1} F_p \\ &= F_n \left(F_p + F_{p-1} \right) + F_{n+1} \left(F_{p+1} + F_p \right) \\ &= F_n F_{p+1} + F_{n+1} F_{p+2} \end{aligned}$$

ce qui est bien ce que l'on désirait.

b) On montre par récurrence que pour tout n, les nombres F_n et F_{n+1} sont premiers entre eux : cela est vrai pour $n = 1$, et l'hérédité s'obtient en remarquant qu'un diviseur commun à F_n et F_{n+1} doit également diviser $F_{n+1} - F_n = F_{n-1}$. La formule prouvée en a) implique alors pour tous p et n, on a $\text{PGCD}\left(F_{n+p}, F_p\right) = \text{PGCD}\left(F_n, F_p\right)$: en effet, un diviseur d commun à F_{n+p} et F_p doit diviser $F_{p-1}F_n$ d'après la formule, mais il est également premier avec F_{p-1} car F_p l'est, et donc le lemme de Gauss assure que d divise F_n ; l'autre sens se traite de façon analogue.

Une récurrence immédiate prouve que si on a une égalité du type $a = bq + r$, alors :

$$\text{PGCD}\left(F_r, F_b\right) = \text{PGCD}\left(F_{b+r}, F_b\right) = \cdots = \text{PGCD}\left(F_{qb+r}, F_b\right) = \text{PGCD}\left(F_a, F_b\right)$$

Le principe de l'algorithme d'Euclide prouve alors que si $d = \text{PGCD}\,(a, b)$, on a $\text{PGCD}\left(F_m, F_n\right) = F_d$.

<u>*Solution de l'exercice 108*</u> : Notons p_k le $(k+1)$-ième nombre premier, de sorte que $p_0 = 2$ désigne le premier nombre premier. Nous allons montrer par récurrence sur n que si $n_d \dots n_0$ est l'écriture de n en base 2 (*ie* si $n = n_0 + 2n_1 + \cdots + 2^d n_d$), alors :

$$x_n = p_0^{n_0} \cdots p_d^{n_d}$$

Pour $n = 0$, c'est vrai. Supposons que ce soit vrai pour n et montrons-le pour $n+1$. Notons $n_d \dots n_0$ l'écriture en base 2 de n. Soit i le plus petit indice tel que $n_i = 0$ (s'il n'existe pas, on convient que $i = d+1$ bien entendu). Dans ce cas, l'écriture en base 2 de $n+1$ est :

$$n_d \dots n_{i+1} \mathtt{1} \mathtt{0} \dots \mathtt{0}$$

D'autre part $p\left(x_n\right) = p_i$ et $q\left(x_n\right) = p_0 \dots p_{i-1}$. On vérifie alors directement l'hypothèse de récurrence.

La factorisation de 111 111 est $3 \times 7 \times 11 \times 13 \times 37$. L'entier n tel que $x_n = 111\,111$ s'écrit en base 2, d'après la propriété que l'on vient de prouver :

$$\mathtt{100000111010}$$

Le nombre cherché est donc 4218.

<u>*Solution de l'exercice 109*</u> : Après certains essais, on constate que f inverse l'écriture en base 2. Plus précisément si a s'écrit en base 2, $a_p \dots a_0$ où a_p est 1, il semble que $f(x)$ soit le nombre qui s'écrive $a_0 \dots a_p$ en base 2

Montrons cela par récurrence. On vérifie que la propriété précédente est vraie aux rangs 1, 2, 3 et 4. Pour l'hérédité supposons que f agisse comme on l'a dit sur les entiers compris entre 1 et n et regardons l'entier $n+1$. Il y a trois cas à distinguer :

Tout d'abord si $n+1$ est pair, alors il s'écrit $2k$ pour un certain entier k. Supposons que k s'écrive $k_p \dots k_0$ en base 2 où k_p vaut $\mathtt{1}$. Alors $2k$ s'écrit :

$$2k \quad : \quad k_p \dots k_0 \mathtt{0}$$

et par hypothèse de récurrence, $f(k)$ s'écrit :

$$f(k) \quad : \quad k_0 \dots k_p$$

ce qui correspond bien à l'écriture renversée. L'hérédité est donc prouvée dans ce cas.

Regardons à présent le cas où $n+1$ s'écrit $4k+1$ pour un certain entier k. Écrivons encore k en base 2 : $k_p \dots k_0$. Alors $4k+1$ s'écrit :

$$4k+1 \quad : \quad k_p \dots k_0 \mathtt{01}$$

et en utilisant l'hypothèse de récurrence on peut poser l'opération suivante :

$$\begin{array}{rrcr} & 2f(2k+1) & : & \mathtt{1}k_0 \dots k_p\mathtt{0} \\ - & f(k) & : & k_0 \dots k_p \\ \hline & & & \mathtt{10}k_0 \dots k_p \end{array}$$

ce qui est bien ce que l'on veut encore une fois.

Finalement si $n+1$ s'écrit $4k+3$ pour un certain entier k. Écrivons encore k en base 2 : $k_p \dots k_0$. Alors $4k+3$ s'écrit :

$$4k+3 \quad : \quad k_p \dots k_0 \mathtt{11}$$

et en utilisant l'hypothèse de récurrence on peut poser l'opération suivante :

$$\begin{array}{rrcr} & 2f(2k+1) & : & \mathtt{1}k_0 \dots k_p\mathtt{0} \\ + & f(2k+1) & : & \mathtt{1}k_0 \dots k_p \\ - & 2f(k) & : & k_0 \dots k_p\mathtt{0} \\ \hline & & & \mathtt{11}k_0 \dots k_p \end{array}$$

la première et la troisième ligne se simplifiant bien. Cela conclut l'hérédité.

Il ne reste plus qu'à compter le nombre d'entiers « symétriques en base 2 » et inférieurs à 1988. Ce nombre en base 2 s'écrit $\mathtt{11111000100}$. Il a onze chiffres.

Avec un seul chiffre, il n'y a qu'une solution ; c'est $\mathtt{1}$. Avec deux chiffres, il n'y a aussi qu'une seule solution ; c'est $\mathtt{11}$. Avec trois chiffres, maintenant, le premier est forcément fixé à $\mathtt{1}$ et par conséquent le dernier aussi, mais on a libre choix sur celui du milieu, il y a donc deux solutions.

De la même façon pour p valant 5, 7 ou 9, il va y avoir $2^{\frac{p-1}{2}}$ solutions de p chiffres. Pour les p pairs, donc valant 4, 6, 8 ou 10, il y aura $2^{\frac{p-2}{2}}$ solutions. Ainsi parmi les nombres qui ont moins de 10 chiffres, on dénombre $1+1+2+2+4+4+8+8+16+16 = 62$ solutions.

Voyons les nombres de 11 chiffres maintenant. Une solution éventuelle doit s'écrire en base 2 sous la forme suivante :

`1_________1`

les cinq premiers « `_` » représentant *a priori* des chiffres arbitraires, et les quatre derniers étant déterminés par le choix des premiers. Toutefois pour que ce nombre reste inférieur à `11111000100`, il faut imposer que les quatre premiers « `_` » ne soient pas simultanément des `1`, et c'est en fait la seule contrainte. On dénombre alors $(2^4 - 1) \times 2 = 30$ solutions dans cette situation.

Au final l'équation proposée admet 92 solutions.

Solution de l'exercice 110 : Montrons d'abord que si $k \leqslant n$, alors le nombre formé par les k derniers chiffres de l'écriture décimale vaut au moins 2^k. En effet, les nombres 2^n et 10^k sont divisibles par 2^k. Il en est donc de même du reste de la division de 2^n par 10^k, qui est justement formé par les k derniers chiffres de 2^n. Ce reste est non nul, et donc on a bien la propriété annoncée.

On note a_i le i-ième chiffre (le chiffre de droite étant le 0-ième) de l'écriture décimale de 2^n. Alors :

$$\begin{aligned} 2^n &= a_0 + 10a_1 + 100a_2 + \cdots + a_i 10^i + \cdots \\ S(2^n) &= a_0 + a_1 + a_2 + \cdots + a_i + \cdots \end{aligned}$$

Soit k tel que $1 \leqslant 4k \leqslant n$. D'après ce que l'on vient de voir, le nombre formé par les chiffres $a_{4k-1} \dots a_1 a_0$ vaut au moins $2^{4k} > 10^k$. Il possède donc au moins un chiffre non nul de rang supérieur ou égal à k. Autrement dit, au moins un parmi $a_k, a_{k+1}, \dots, a_{4k-1}$ est non nul.

Soit $n \geqslant 4$ un entier, et soit m tel que $4^m \leqslant n < 4^{m+1}$. Chacun des intervalles $[1,3], [4,15], \dots, [4^{m-1}, 4^m - 1]$ contient donc au moins un entier i tel que $a_i \neq 0$. On en déduit que :

$$S(2^n) \geqslant m \geqslant \log_4 n - 1$$

ce qui permet de conclure.

5.3 Exercices de « *Congruences* »

Solution de l'exercice 111 : Pour voir que le produit de k entiers consécutifs positifs n, $n+1$, …, $n+k-1$ est divisible par $k!$, il suffit de remarquer que :

$$\frac{n(n+1)\cdots(n+k-1)}{k!} = C_n^k$$

est entier. S'ils sont tous négatifs, on considére les opposés. Sinon, c'est que l'un d'entre eux est nul, et donc le produit également.

Solution de l'exercice 112 : Soit $n = n_r \dots n_1 n_0$ l'écriture de n en base 2. Pour tout k, si $k = k_r \dots k_1 k_0$ en base 2, on a :

$$C_n^k \equiv \prod_{i=0}^{r} C_{n_i}^{k_i} \pmod 2$$

donc C_n^k est impair si et seulement si $C_{n_i}^{k_i} = 1$ pour tout i, c'est-à-dire lorsque l'on a pas, pour un certain i, $k_i = 1$ et $n_i = 0$.

Cette condition est automatiquement vérifiée si tous les n_i sont égaux à 1, et réciproquement, si l'on a $n_j = 0$ pour un certain $j \leqslant r$, alors en prenant $k = 2^j < n$, il vient que C_n^k est pair.

Finalement, C_n^k est impair pour $0 \leqslant k \leqslant n$ si et seulement si tous les chiffres de l'écriture en base 2 de n valent 1, ce qui revient à dire que n est de la forme $2^{r+1} - 1$.

Solution de l'exercice 113 : Notons k le nombre de suites et pour i compris entre 1 et k, notons N_i la raison de la i-ième suite et a_i un de ses termes. L'ensemble des valeurs prises par la i-ième suite est alors l'ensemble des entiers x tels que :

$$x \equiv a_i \pmod{N_i}$$

Il s'agit donc de prouver que le système suivant :

$$(S) : \left\{ \begin{array}{rcll} x & \equiv & a_1 & \pmod{N_1} \\ x & \equiv & a_2 & \pmod{N_2} \\ & \vdots & & \\ x & \equiv & a_k & \pmod{N_k} \end{array} \right.$$

admet une solution. Mais pour cela, on a vu dans le cours qu'il suffit de vérifier que pour tous i et j, on a $a_i \equiv a_j \pmod{\text{PGCD}(N_i, N_j)}$. Or cela est vrai, puisque par hypothèse, le système formé par les i-ième et j-ième lignes de (S) admet une solution.

Solution de l'exercice 114 : Pour tout d diviseur de n, notons A_d l'ensemble des éléments de $\{1, \dots, n\}$ dont le PGCD avec n faut exactement $\frac{n}{d}$.

Déjà, il est évident que les A_d sont deux à deux disjoints et que leur réunion est égale à tout $\{1, \dots, n\}$, puisque pour tout $i \in \{1, \dots, n\}$, le PGCD de n et de i est un nombre de la forme $\frac{n}{d}$ pour d un diviseur de n.

Soit $x \in A_d$. L'entier $\frac{xd}{n}$ est un élément de $\{1, \dots, d\}$ et il est premier avec d. Réciproquement, tous les éléments de A_d sont obtenus ainsi. Il s'ensuit que $\text{Card}\, A_d = \varphi(d)$. La conclusion découle de tout ce qui précède.

Solution de l'exercice 115 : C'est en fait une application du théorème chinois[9]. Appelons x le nombre de soldats. La méthode des chinois permet au général d'accéder à des nombres x_2, x_3, x_5, x_7, x_{11}, x_{13} et x_{17} tels que :

$$x \equiv x_i \pmod{i}$$

pour tout $i \in \{2, 3, 5, 7, 11, 13, 17\}$. On constate que les nombres de l'ensemble précédent sont premiers entre eux deux à deux, et donc le théorème chinois s'applique et affirme qu'il existe un entier n tel que le système précédent soit également à :

$$x \equiv n \pmod{510\,510}$$

[9]D'où le nom...

On conclut en remarquant qu'il existe au plus un entier inférieur à 500 000 et satisfaisant cette dernière congruence.

<u>*Solution de l'exercice 116*</u> : Dans un premier temps, on remarque que $a = b^n$ est bien solution du problème.

Supposons qu'il y ait deux solutions, disons a et a'. Soit $k > b$ un entier. Les nombres $a - k^n$ et $a' - k^n$ doivent tous deux être divisibles par $b - k$ et donc en particulier congrus modulo $b-k$. On en déduit que pour tout $k > b$, on doit avoir $a \equiv a' \pmod{b-k}$. Autrement dit, a et a' doivent être congrus modulo tous les entiers strictement positifs. Mais cela n'est possible que si $a = a'$. D'où la conclusion.

<u>*Solution de l'exercice 117*</u> : Cet exercice est évident avec les congruences. Comme $9 \equiv 2 \pmod 7$, on a $9^n \equiv 2^n \pmod 7$ pour tout n, ce qui est bien ce que l'on veut. Si l'on préfère, on peut également utiliser la factorisation :

$$9^n - 2^n = (9-2)\left(9^{n-1} + 9^{n-2} \cdot 2 + \cdots + 2^{n-1}\right)$$

qui permet de conclure directement également.

<u>*Solution de l'exercice 118*</u> : On a les congruences $4p+1 \equiv p+1 \pmod 3$ et $7p-4 \equiv p+2 \pmod 3$. Ainsi forcément l'un des trois nombres p, $4p+1$ et $7p-4$ est un multiple de 3. Comme $4p+13$ et $7p-4$ sont tous les deux forcément strictement supérieur à 3, c'est forcément p le multiple de 3 et puis $p = 3$.

On vérifie réciproquement que pour $p = 3$, on a $4p+1 = 12$ et $7p-4 = 17$ qui sont bien tous premiers.

<u>*Solution de l'exercice 119*</u> : Non. Supposons qu'une telle permutation existe. Des deux égalités :

$$\begin{array}{rcl} a_i + \cdots + a_{i+9} & \equiv & 0 \pmod{10} \\ a_{i+1} + \cdots + a_{i+10} & \equiv & 0 \pmod{10} \end{array}$$

on déduit $a_i \equiv a_{i+10} \pmod{10}$ pour tout i pour lequel cela a un sens. Comme les a_i doivent atteindre tous les résidus modulo 10, on en déduit qu'il en est de même de l'ensemble $\{a_1, \ldots, a_{10}\}$.

Mais cet ensemble a dix éléments, et il y a dix résidus modulo 10 et donc $\{a_1, \ldots, a_{10}\}$ doit être une permutation modulo 10 de l'ensemble $\{1, \ldots, 10\}$. En particulier, on doit avoir :

$$a_1 + \cdots + a_{10} \equiv 1 + \cdots + 10 \equiv 5 \pmod{10}$$

ce n'est pas en accord avec l'hypothèse.

<u>*Solution de l'exercice 120*</u> : Un point A de coordonnées entières (x, y) est invisible si et seulement si $\text{PGCD}\,(x, y) > 1$. On cherche donc des entiers x et y tels que pour tous entiers i et j dans $\{0, \ldots, L\}$, les nombres $x+i$ et $y+j$ ne soient pas premiers entre eux. (Le point (x, y) sera alors le coin inférieur gauche d'un carré convenable).

Considérons, pour i et j variant entre 0 et L, des nombres premiers p_{ij} deux à deux distincts. D'après le lemme chinois, il existe un entier x tel que $x \equiv -i \pmod{p_{ij}}$ pour tous i et j. De même il existe un entier y tel que $y \equiv -j \pmod{p_{ij}}$ pour tous i et j.

Pour un tel choix d'entiers, on a bien p_{ij} divise à la fois $x+i$ et $y+j$.

Solution de l'exercice 121 : Il suffit de reconnaître les coefficients binomiaux C_4^k dans l'écriture de 104060401 :

$$104060401 = \sum_{k=0}^{4} C_4^k 10^{2k} = 101^4$$

Or 101 est premier, donc les diviseurs de 101^4 sont les 101^k, $0 \leqslant k \leqslant 4$. Ainsi :

$$\sigma(104060401) = \frac{101^5 - 1}{100} = \frac{10510100501 - 1}{100} = 105101005$$

Solution de l'exercice 122 : Notons S la somme envisagée. On écrit :

$$\begin{aligned} 2S &= \left(1 + \frac{1}{p-1}\right) + \left(\frac{1}{2} + \frac{1}{p-2}\right) + \cdots + \left(\frac{1}{i} + \frac{1}{p-i}\right) + \cdots + \left(\frac{1}{p-1} + 1\right) \\ &= p\left[\frac{1}{p-1} + \cdots + \frac{1}{i\,(p-i)} + \cdots + \frac{1}{p-1}\right] \end{aligned}$$

Le terme entre crochets est représentée par une fraction dont le dénominateur est premier à p. Ceci termine l'exercice.

Solution de l'exercice 123 : Notons 2^n et 2^m, avec $n < m$, deux éventuelles puissances de 2 ayant exactement les mêmes chiffres. En particulier 2^n et 2^m ont le même nombre de chiffres et donc $m - n < 4$. La différence $m - n$ vaut donc 1, 2 ou 3.

D'autre part, on doit avoir $2^n \equiv 2^m \pmod 9$, soit $2^{m-n} \equiv 1 \pmod 9$. Mais on vérifie que $2^1 \equiv 2 \pmod 9$, $2^2 \equiv 4 \pmod 9$ et $2^3 \equiv 8 \pmod 9$. Aucun ne vaut 1, il n'y a donc pas de solution.

Solution de l'exercice 124 : Soit $n = n_r \dots n_1 n_0$ et $k = k_r \dots k_1 k_0$ les écritures de n et k en base 2. Dans la solution de l'exercice 5.3, on a vu que C_n^k était impair si et seulement si pour tout i tel que $n_i = 0$, on avait $k_i = 0$. Par conséquent, si n a s zéros dans son écriture binaire, il en résulte que le nombre d'entiers k compris entre 0 et n qui conviennent est exactement 2^{r+1-s}. En particulier, c'est bien une puissance de 2.

Solution de l'exercice 125 : S'il existait une telle suite, elle contiendrait à l'évidence un nombre premier strictement supérieur à 7. On peut donc supposer $x_0 = p > 7$. Un tel p est forcément congru à 1 ou 5 modulo 6.

Supposons $p \equiv 1 \pmod 6$. Alors $2p+1 \equiv 3 \pmod 6$ et donc $2p+1$ est un multiple de 3. Ainsi on a forcément $x_1 = 2p-1$. En outre $2p-1 \equiv 1 \pmod 6$, et en appliquant à nouveau le même raisonnement, il vient $x_2 = 2x_1 - 1$. Par récurrence, on prouve que $x_n = 2x_{n-1} - 1$, ce qui donne la formule générale :

$$x_n = 2^n p - 2^n + 1$$

Mais alors $x_{p-1} = 2^{p-1}p - 2^{p-1} + 1 \equiv 0 \pmod p$ d'après le petit théorème de Fermat. Ceci constitue une contradiction.

On traite de même le cas où $p \equiv 5 \pmod 6$.

<u>*Solution de l'exercice 126*</u> : La réponse est affirmative. Pour construire une telle permutation, on commence par poser $a_1 = 1$. Soit ensuite $k \geqslant 1$ fixé. Supposons que l'on ait déterminé des entiers strictement positifs deux à deux distincts $a_1, \cdots, a_k$ tels que pour tout $i \leqslant k$ on ait :

$$\sum_{j=1}^{i} a_j = 0 \pmod i$$

Soit alors n le plus petit entier non encore utilisé. Puisque $k+1$ et $k+2$ sont premiers entre eux, le lemme chinois assure de l'existence d'un entier m arbitrairement grand, et donc différent de n et de chacun des a_i déjà choisis, tel que :

$$\begin{aligned} m &\equiv -(a_1 + \cdots + a_k) \pmod{k+1} \\ m &\equiv -(a_1 + \cdots a_k + n) \pmod{k+2} \end{aligned}$$

On pose alors $a_{k+1} = m$ et $a_{k+2} = n$. La suite ainsi construite vérifie clairement la condition de divisiblité, et la minimalité du n considéré à chaque étape assure que l'on utilisera bien chaque entier une et une seule fois.

<u>*Solution de l'exercice 127*</u> : Notons $x_1, \ldots, x_{111}$ nos entiers. Ils sont tels que $x_1 + \cdots + x_{111} = 0$. Dans un premier temps on remarque que $399 = 3 \times 7 \times 19$. Nous allons donc montrer que le nombre :

$$x_1^{37} + \cdots + x_{111}^{37}$$

est à la fois multiple de 3, 7 et 19. Par le petit théorème de Fermat, on a $x^2 \equiv 1 \pmod 3$ pour tout x premier avec 3. En élévant à la puissance 18, on obtient $x^{36} \equiv 1 \pmod 3$, puis $x^{37} \equiv x \pmod 3$, cette dernière congruence étant en fait valable pour tout x. Ainsi :

$$x_1^{37} + \cdots + x_{111}^{37} \equiv x_1 + \ldots + x_{111} = 0 \pmod 3$$

On raisonne de la même façon dans les autres cas.

<u>*Solution de l'exercice 128*</u> : On a :

$$\begin{aligned} & 1 - \tfrac{1}{2} + \tfrac{1}{3} - \tfrac{1}{4} + \cdots - \tfrac{1}{1318} + \tfrac{1}{1319} \\ & = \left(1 + \tfrac{1}{2} + \cdots + \tfrac{1}{1319}\right) - 2\left(\tfrac{1}{2} + \tfrac{1}{4} + \cdots + \tfrac{1}{1318}\right) \\ & = \left(1 + \tfrac{1}{2} + \cdots + \tfrac{1}{1319}\right) - \left(1 + \tfrac{1}{2} + \cdots + \tfrac{1}{659}\right) \\ & = \tfrac{1}{660} + \cdots + \tfrac{1}{1319} \end{aligned}$$

On a $\frac{1}{660} + \frac{1}{1319} = \frac{1979}{660 \times 1319}$ et ainsi de suite. Comme la somme précédente comporte un nombre pair de termes, on obtient au final :

$$1979 \left[\frac{1}{660 \times 1319} + \frac{1}{661 \times 1318} + \cdots + \frac{1}{989 \times 990} \right]$$

Le terme entre crochets est une fraction dont le dénominateur est premier avec 1979 (car 1979 est premier). On a donc obtenu une écriture de la somme sous la forme $\frac{a'}{b'}$ avec a'

multiple de 1979 et b' premier avec 1979. Si $\frac{a}{b}$ est une autre écriture, on a l'égalité $ab' = b'a$ et donc 1979 divise ab', puis a par le lemme de Gauss.

Remarque. Si l'on sait que les fractions dont le dénominateur premier avec p peuvent se voir dans $\mathbf{Z}/p\mathbf{Z}$ (voir la seconde partie, chapitre 5), on peut procéder différemment. La somme S que l'on cherche à estimer est :

$$1 + \frac{1}{2} + \cdots + \frac{1}{1319} + \frac{1}{-1} + \frac{1}{-2} + \cdots + \frac{1}{-659}$$

et l'on remarque qu'il s'agit de la somme des inverse des entiers : $-659 \equiv 1320 \pmod p$, $-658 \equiv 1321 \pmod p$ et ainsi de suite. On conclut alors en utilisant l'exercice 5.3.

<u>*Solution de l'exercice 129*</u> : Un nombre premier p convenable s'écrit :

$$p = p_0 + p_1 b + \cdots + p_{b-1} b^{b-1}$$

où $(p_0, \ldots, p_{b-1})$ est une permutation de l'ensemble $\{0, \ldots, b-1\}$. On a alors :

$$p \equiv 0 + 1 + \cdots + (b-1) = \frac{b\,(b-1)}{2} \pmod{b-1}$$

et donc si b est pair, p est un multiple de $b-1$. Si $b > 2$, p a au moins deux chiffres non nuls et donc $p > b-1$. Ceci prouve que p ne peut-être un nombre premier. Pour $b = 2$, on voit directement que le nombre s'écrivant `01` en base 2 (*i.e.* 1) n'est pas premier, alors que celui s'écrivant `10` (*i.e.* 2) l'est.

Si b est impair, on pose $n = \frac{b-1}{2}$. On a $b \equiv 1 \pmod n$ et donc :

$$p \equiv 0 + 1 + \cdots + (b-1) = \frac{b\,(b-1)}{2} \equiv 0 \pmod n$$

Or si $b > 3$, on a comme précédemment $p > n$, ce qui est contradictoire car p est premier. Il ne reste plus qu'à vérifier pour les nombres écrits en base 3. Il y a `012` (5), `021` (7), `102` (11), `120` (15), `201` (19) et `210` (21).

Finalement les nombres premiers p qui conviennent sont 2, 5, 7, 11 et 19.

<u>*Solution de l'exercice 130*</u> : Il suffit de prouver que pour tout d, $2d-1$, $5d-1$ ou $13d-1$ n'est pas un carré. Supposons qu'ils soient tous les trois des carrés. Comme $2d-1$ est impair, il faut qu'il soit congru à 1 modulo 4, et donc d doit être impair. On pose $d = 2d' + 1$. Comme $2d-1 = 4d'+1$ est congru à 1 modulo 4, il doit être congru à 1 modulo 8, et donc d' est pair. On pose donc $d' = 2d''$ et ainsi les deux nombres $20d'' + 4$ et $52d'' + 12$ sont des carrés. Ces deux nombres sont congrus respectivement à $4d'' + 4$ et $4d'' + 12$ modulo 16. On obtient une contradiction en remarquant que les seuls résidus quadratiques multiples de 4 modulo 16 sont 0 et 4 ; ils ne peuvent donc différer de 8.

<u>*Solution de l'exercice 131*</u> : Non, un tel entier n'existe pas. En effet, supposons qu'il existe. Dans un premier temps, on constate qu'au plus un nombre de l'ensemble $\{n, \ldots, n+18\}$ peut être un multiple de 19. Ainsi s'il y a un tel élément, il sera soit dans A, soit dans B. Supposons que ce soit dans A. Alors 19 divise le produit des éléments de A mais pas celui des éléments de B puisqu'il est premier. C'est une contradiction.

On en déduit qu'aucun élément n'est multiple de 19. Ainsi modulo 19, l'ensemble $\{n, \ldots, n+18\}$ est exactement l'ensemble $\{1, \ldots, 18\}$. Si l'on note P le produit des éléments de A (qui est aussi celui des éléments de B), on a donc :

$$P^2 \equiv 1 \times 2 \times \ldots \times 18 \pmod{19}$$

et d'après le théorème de Wilson (ou un calcul si on ne connaît pas ce théorème), $P^2 \equiv -1 \pmod{19}$. Mais en calculant tous les résidus quadratiques modulo 19, on vérifie que cette congruence est impossible.

<u>*Solution de l'exercice 132*</u> : Le nombre $|B^2-1|-(B^2-1)$ est non nul si, et seulement si $B^2-1<0$, c'est-à-dire puisque B est un entier si, et seulement si $B=0$. Ainsi si $B \neq 0$, on a toujours $f(x,y)=2$ qui est premier.

Si $B=0$, on a $|B^2-1|-(B^2-1)=2$ et $f(x,y)=y+1$. Le fait que B soit nul implique $y!+1=x(y+1)$, soit encore $y! \equiv -1 \pmod{y+1}$, ce qui assure, d'après le théorème de Wilson, que $y+1=f(x,y)$ est premier. Ainsi la fonction f ne prend que des valeurs qui sont des nombres premiers.

Considérons à présent p un nombre premier impair. D'après ce qu'il précède, s'il s'écrit $f(x,y)$, c'est que $y=p-1$ et que $y!+1=x(y+1)$, soit $x=\frac{(p-1)!+1}{p}$. Le nombre premier p ne peut donc être atteint qu'une unique fois. Et il est effectivement atteint, lorsque l'on choisit x et y comme précédemment : la fraction qui définit x est bien un entier, encore d'après le théorème de Wilson.

<u>*Solution de l'exercice 133*</u> : Soit p un nombre premier différent de 2 et de 5. Alors parmi les nombres $n, n+1, \ldots, n+p-1$, il y en a un et un seul qui est un multiple de p. Autrement dit, il existe un unique entier $k \in \{n, n+1, \ldots, n+p-1\}$ tel que $v_p(k) \geqslant 1$. Pour les autres, on a $v_p(k)=0$. Cela prouve que :

$$v_p\left(\frac{1}{n}+\frac{1}{n+1}+\cdots+\frac{1}{n+p-1}\right) \leqslant -1$$

Un nombre décimal est un nombre de la forme $\frac{a}{10^s}$. En tout cas, sa valuation p-adique (pour p différent de 2 et 5) est nulle. Cela résout la première partie de la question.

Traitons maintenant le cas $p=2$. Si ℓ est un nombre premier différent de 2 et 5, par le même argument que précédemment, on prouve qu'aucun des deux nombres n et $n+1$ ne peut être multiple de ℓ. Il en résulte que l'on peut écrire $n+1=2^a5^b$ et $n=2^{a'}5^{b'}$, pour des entiers a, b, a' et b' positifs ou nuls. On est donc amené à considérer l'équation :

$$2^a5^b = 2^{a'}5^{b'}+1$$

Si on a $a>0$, alors le membre de gauche de l'égalité précédente est pair. Pour que le membre de droite le soit aussi, il faut $a'=0$. De même on prouve que si $b>0$, alors on doit avoir $b'=0$ et des énoncés analogues en échangeant soit a et a', soit b et b' soit les deux. Bref, on est ramené à résoudre séparément les deux équations suivantes :

$$2^a = 5^{b'}+1 \quad \text{et} \quad 5^b = 2^{a'}+1$$

Pour la première équation, on regarde modulo 4 : si $a \geqslant 2$, le terme de gauche vaut toujours 0 et celui de droite toujours 1. On a donc forcément $a = 1$ (car $a = 0$ ne convient pas) et donc $b' = 0$. Regardons l'autre équation. On vérifie d'abord que $a' = 1$ ne fournit aucune solution, contrairement à $a' = 2$ qui donne $b = 1$. Ensuite, on regarde l'équation modulo 3 : on obtient $2^b \equiv 2^{a'} + 1 \pmod 3$, ce qui n'est possible que si b est impair. Posons $b = 2u + 1$. L'équation devient :

$$5 \times 25^u = 2^{a'} + 1$$

Maintenant si $a' \geqslant 3$, on a $2^{a'}+1 \pmod 8$, mais $5 \times 25^u \equiv 5 \pmod 8$, d'où une contradiction. Finalement, les seuls nombres consécutifs de la forme $2^x 5^y$ sont d'une part 1 et 2 et d'autre part 4 et 5. On en déduit que les seules sommes qui conviennent sont :

$$1 + \frac{1}{2} = 1,5 \quad \text{et} \quad \frac{1}{4} + \frac{1}{5} = 0,45$$

Reste le cas $p = 5$. Comme pour le cas $p = 2$, on montre qu'il n'est pas possible qu'un nombre premier $\ell > 5$ divise un des nombres n, $n+1$, $n+2$, $n+3$ et $n+4$. D'autre part, encore par le même argument, on montre que 3 doit forcément diviser deux nombres de la liste précédente, donc soit n et $n+3$, soit $n+1$ et $n+4$. Quoi qu'il en soit, les deux nombres intermédiaires sont consécutifs et non divisibles par 3 et donc de la forme $2^x 5^y$. De l'étude faite précédemment, on déduit facilement que la seule solution est :

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} = 1,45$$

Solution de l'exercice 134 : **a)** Soit $n > 0$ un entier. On pose $M_n = \{a_1, \ldots, a_n\}$ où $a_k = (k \cdot n!)^{n!}$ pour tout k. Soit $r \in \{1, \ldots, n\}$. On note que chacun des a_k est un entier strictement positif divisible par r et que c'est également une puissance r-ième d'entier. Cela assure que la somme de r quelconques d'entre eux est un multiple de r et que le produit de r quelconques d'entre eux est une puissance r-ième, et donc que l'ensemble M_n convient.

b) Non. On raisonne par l'absurde en supposant qu'un tel ensemble infini existe. Appelons-le M. Soient a et b deux éléments de M, distincts. Alors, il existe un nombre premier p qui ne divise pas $a - b$. Soient $x_1, x_2, \cdots, x_{p-1}$ des éléments de $M \backslash \{a, b\}$ deux à deux distincts. Alors :

$$\begin{aligned} x_1 + \cdots + x_{p-1} + a &\equiv 0 \pmod p \\ x_1 + \cdots + x_{p-1} + b &\equiv 0 \pmod p \end{aligned}$$

Mais alors $a \equiv b \pmod p$, ce qui est supposé faux.

Solution de l'exercice 135 : Si $u_n > 7$, soit u_n est pair et $u_{n+1} = \frac{u_n}{2}$ est inférieur à u_n. Soit u_n est impair, $u_{n+1} = u_n + 7$ est pair, donc $u_{n+2} = \frac{u_n+7}{2} < u_n$. Il en résulte que la plus petite valeur ne peut pas être strictement supérieure à 7. Mais elle peut être égale à 7, car si $u_n = 7$, les termes suivants sont $14, 7, 14, 7, \ldots$ et la suite ne descend plus. Si $u_n = 2$, 4 ou 6, alors $u_{n+1} = \frac{u_n}{2}$ est strictement inférieur à u_n. Si $u_n = 5$, les termes suivants sont $12, 6, 3, 10, 5, 12, \ldots$ et la suite descend jusqu'à 3. De même si $u_n = 3$. Enfin, si $u_n = 1$, u_n

ne peut pas descendre plus bas, les termes suivants de la suite étant $8, 4, 2, 1, 8, 4, \ldots$. Le plus petit entier atteint par cette suite peut être soit 1, soit 3, soit 7, tout dépend quel est le nombre de départ.

Pour atteindre 7, il faut que tous les termes de la suite soient multiples de 7, car u_{n+1} est divisible par 7 si et seulement si u_n est divisible par 7. Or il est clair que 2000^{2003} n'est pas multiple de 7 car 2000 n'est pas multiple de 7. Plus précisément, $2000 \equiv 5 \pmod 7$, car $1995 = 7 \times 285$. On a $5^2 \equiv 4 \pmod 7$, $5^3 \equiv 6 \pmod 7$, $5^4 \equiv 2 \pmod 7$, $5^5 \equiv 3 \pmod 7$ et (comme permettait de le prévoir le théorème de Fermat) $5^6 \equiv 1 \pmod 7$. Pour tout k, 5^{6k} sera donc congru à 1 modulo 7, en particulier 5^{1998} (puisque $1998 = 6 \times 333$). D'où 5^{2003} est congru à 3 modulo 7, puisque $2003 = 1998 + 5$. Il en résulte que $2000^{2003} \equiv 3 \pmod 7$.

Or l'algorithme transforme un nombre congru à 3 modulo 7 :
– s'il est impair, en un autre nombre congru à 3 modulo 7 (puisqu'on ajoute 7)
– s'il est pair, en un nombre congru à 5 modulo 7 (puisque 2×5 congru à 3 modulo 7)

Un nombre congru à 5 modulo 7 est transformé, s'il est impair, en un autre nombre congru à 5 modulo 7, et s'il est pair, en un nombre congru à 6 modulo 7. Un nombre congru à 6 modulo 7 est transformé, s'il est impair, en un autre nombre congru à 6 modulo 7, et s'il est pair, en un nombre congru à 3 modulo 7.

La boucle est bouclée : à partir d'un nombre congru à 3 modulo 7, en réitérant autant de fois que l'on veut l'algorithme, on ne peut obtenir que des nombres congrus à 5, 6 ou 3 modulo 7. On ne peut donc jamais atteindre le nombre 1 : le plus petit entier atteint par cette suite est 3.

Solution de l'exercice 136 : Soit p un nombre premier quelconque. La valuation p-adique de $a_n = \text{PPCM}(1, 2, \ldots, 2n)$ est le plus grand entier v tel que $p^v \leqslant 2n$. Mais alors pour tout $k > v$, on a :

$$\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right] = 0$$

Par conséquent, on a :

$$\begin{aligned} v_p(C_{2n}^n) &= \sum_{k \geqslant 1} \left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right] \\ &= \sum_{k=1}^{v} \left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right] \\ &\leqslant \sum_{k=1}^{v} 1 = v \quad (\text{puisque } [2x] \leqslant 2[x] + 1) \end{aligned}$$

On a donc montré que pour tout nombre premier, $v_p(C_{2n}^n) \leqslant v_p(a_n)$, ce qui assure que C_{2n}^n divise a_n.

Solution de l'exercice 137 : Soit ℓ un diviseur premier de $p^p - 1$. On a alors $p^p \equiv 1 \pmod \ell$. D'après le petit théorème de Fermat, on a $p^{\ell-1} \equiv 1 \pmod \ell$ et donc l'ordre de p modulo ℓ est un diviseur de $\text{PGCD}(p, \ell - 1)$. C'est soit 1, soit p.

Si c'est p, comme $p^{\ell-1} \equiv 1 \pmod \ell$, il vient p divise $\ell - 1$ et donc $\ell \equiv 1 \pmod p$ comme on le veut.

Si c'est 1 cela signifie que $p \equiv 1 \pmod{\ell}$, c'est-à-dire que ℓ divise $p-1$.

Il suffit donc de prouver qu'il existe un diviseur premier ℓ pour lequel cet ordre est p, c'est-à-dire ne divisant pas $p-1$. Pour cela, on introduit la factorisation :

$$p^p - 1 = (p-1)\left[p^{p-1} + p^{p-2} + \cdots + p + 1\right]$$

Le facteur entre crochets est congru à 1 modulo $p-1$ et donc est premier avec $p-1$. Ainsi tout nombre premier ℓ divisant ce facteur est un diviseur premier de p^p-1 ne divisant pas $p-1$. Il ne reste plus qu'à prouver que ce facteur est strictement supérieur à 1 mais c'est évident.

Solution de l'exercice 138 : Le quotient :

$$\frac{(n_1 + \cdots + n_k)!}{n_1! \cdots n_k!}$$

peut se voir comme le nombre de partitions ordonnées $(E_1, \ldots, E_k)$ d'un ensemble E à $n_1 + \cdots + n_k$ éléments en k ensembles E_1, ..., E_k, avec $\operatorname{Card} E_i = n_i$. Il en résulte en particulier que c'est un entier.

Remarque. On laisse au lecteur le soin de traiter cet exercice par les valuations p-adiques.

Solution de l'exercice 139 : Soit p un nombre premier quelconque. On veut voir que $v_p(C_{2n}^n) \geqslant v_p(n+1)$. Pour cela, notons $\ell = v_p(n+1)$. Ainsi $n+1$ s'écrit $p^\ell m$ avec m premier à p. Si $\ell = 0$ le résultat est clair. Sinon, on remarque que pour $1 \leqslant k \leqslant \ell$, on a :

$$\left[\frac{n}{p^k}\right] = \left[p^{\ell-k}m - \frac{1}{p^k}\right] = p^{\ell-k}m - 1$$

et de même :

$$\left[\frac{2n}{p^k}\right] = \left[2p^{\ell-k}m - \frac{2}{p^k}\right] = 2p^{\ell-k}m - 1$$

car $p^k \geqslant 2$. Par conséquent, on a la minoration suivante de $v_p(C_{2n}^n)$:

$$\begin{aligned} v_p(C_{2n}^n) &= \sum_{k \geqslant 1} \left(\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right] \right) \\ &\geqslant \sum_{k=1}^{\ell} \left(\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right] \right) \\ &\geqslant \sum_{k=1}^{\ell} 1 = \ell \end{aligned}$$

ce qui conclut.

Autre solution. Un calcul prouve que :

$$\frac{1}{n+1} \mathrm{C}_{2n}^n = \mathrm{C}_{2n}^n - \mathrm{C}_{2n}^{n+1}$$

et voilà...

Remarque. L'entier $c_n = \frac{1}{n+1} C_{2n}^n$ s'appelle le n-ième nombre de Catalan. Il apparaît dans un certain nombre de problème de dénombrement. Par exemple, c'est le nombre de bons parenthésages que l'on peut faire avec n parenthèses ouvrantes et n parenthèses fermantes.

Solution de l'exercice 140 : On calcule les puissances successives de 3 modulo 17 :

$$3^0 \equiv 1 \pmod{17} \quad ; \quad 3^1 \equiv 3 \pmod{17} \quad ; \quad 3^2 \equiv 9 \pmod{17}$$

$$3^3 \equiv -7 \pmod{17} \quad ; \quad 3^4 \equiv -4 \pmod{17} \quad ; \quad 3^5 \equiv 5 \pmod{17}$$
$$3^6 \equiv -2 \pmod{17} \quad ; \quad 3^7 \equiv -6 \pmod{17} \quad ; \quad 3^8 \equiv -1 \pmod{17}$$
$$3^9 \equiv -3 \pmod{17} \quad ; \quad 3^{10} \equiv -9 \pmod{17} \quad ; \quad 3^{11} \equiv 7 \pmod{17}$$
$$3^{12} \equiv 4 \pmod{17} \quad ; \quad 3^{13} \equiv -5 \pmod{17} \quad ; \quad 3^{14} \equiv 2 \pmod{17}$$
$$3^{15} \equiv 6 \pmod{17} \quad ; \quad 3^{16} \equiv 1 \pmod{17} \quad ; \quad 3^{17} \equiv 3 \pmod{17}$$

La suite obtenue est périodique de période 16. On raisonne alors comme suit. Si $n \equiv 0 \pmod{16}$, alors $3^n \equiv 1 \pmod{17}$, et donc on doit avoir $n \equiv -16 \pmod{272}$ d'après le lemme chinois.

Si $n \equiv 1 \pmod{16}$, alors $3^n \equiv 3 \pmod{17}$ et donc on doit avoir $n \equiv -31 \pmod{272}$.

On traite ainsi tous les cas. Toutes les solutions trouvées précédemment conviennent comme on le vérifie immédiatement.

Finalement les solutions sont les entiers congrus à -16, -31, 162, 163, 132, 5, 134, 57, 152, -71, 42, 75, 140, 29, -66 ou -33 modulo 272 (sauf erreur !).

Remarque. Pour accélérer les calculs, on peut remarquer que le nombre $17a - 16b$ est congru à a modulo 16 et à b modulo 17.

Solution de l'exercice 141 : Pour montrer que :

$$a(m, n) = \frac{(2m)!(2n)!}{n!m!(m+n)!}$$

est entier, on peut par exemple procéder par récurrence sur n. En effet, $a(m, 0) = C_{2m}^m$ est entier pour tout m. Supposons que pour un certain n, $a(m, n)$ soit entier pour tout n, et remarquons que l'on a :

$$a(m, n+1) = \frac{2(n+1)(2n+1)(2m)!(2n)!}{(n+1)(m+n+1)m!n!(m+n)!} = \frac{2(2n+1)}{m+n+1} a(m, n)$$

On a de plus la relation symétrique en échangeant m et n, si bien que :

$$a(m+1, n) + a(m, n+1) = \frac{2(2n+1) + 2(2m+1)}{m+n+1} a(m, n) = 4a(m, n)$$

Ainsi $a(m, n+1) = 4a(m, n) - a(m+1, n)$ est entier d'après l'hypothèse de récurrence.

Finalement, on a bien montré que $a(m,n)$ était entier pour tous m, n. Notons que l'on aurait également pu conclure en établissant la positivité de $v_p(a(m,n))$ pour tout nombre premier p.

Solution de l'exercice 142 : Supposons que $n_1, \ldots, n_k$ forment une solution. Clairement, si l'un des n_i est égal à 1, on en déduit par réaction en chaîne que tous sont égaux à 1.

On suppose donc qu'aucun des n_i n'est égal à 1. Pour tout i, on note p_i le plus petit diviseur premier de n_i. Alors p_i divise $2^{n_{i-1}} - 1$ (avec $n_0 = n_k$). Notons que cela assure en passant que p_i est impair. Soit m_i l'ordre de 2 modulo p_i. Alors m_i divise n_{i-1} et m_i divise $p_i - 1$ (d'après le petit théorème de Fermat). En particulier, $1 < m_i \leqslant p_i - 1 < p_i$ et donc le plus petit diviseur p_{i-1} de n_{i-1} est inférieur à p_i. D'où $p_k > p_{k-1} > \cdots > p_1 > p_k$. Il n'y a donc bien pas d'autre solution.

Solution de l'exercice 143 : On commence par calculer la suite des puissances de 7 modulo 43. On obtient :

$$7^0 \equiv 1 \pmod{43} \quad ; \quad 7^1 \equiv 7 \pmod{43} \quad ; \quad 7^2 \equiv 6 \pmod{43}$$

$$7^3 \equiv -1 \pmod{43} \quad ; \quad 7^4 \equiv -7 \pmod{43}$$

$$7^5 \equiv -6 \pmod{43} \quad ; \quad 7^6 \equiv 1 \pmod{43}$$

La suite est donc périodique de période 6. De plus, on constate que $7^2 \equiv 6 \pmod{43}$ et donc la suite des puissances de 6 est périodique de période 3. Un nombre premier $p \geqslant 5$ est congru soit à 1, soit à 5 modulo 6.

Si $p \equiv 1 \pmod 6$, on a $7^p \equiv 7 \pmod{43}$ et $6^p \equiv 6 \pmod{43}$ et donc $7^p - 6^p - 1$ est un multiple de 43. Si $p \equiv 5 \pmod 6$, on a $7^p \equiv -6 \pmod{43}$ et $6^p \equiv -7 \pmod{43}$ et donc $7^p - 6^p - 1$ est aussi un multiple de 43. Cela conclut.

Solution de l'exercice 144 : Posons $N = 2^b - 1$. Alors évidemment, $2^b \equiv 1 \pmod N$. Soit r le reste de la division euclidienne de a par b. On a alors $a \equiv r \pmod b$ et donc $2^a \equiv 2^r \pmod N$.

Ainsi si N divise $2^a + 1$, il divise également $2^r + 1$. Mais si $b > 2$, on a forcément, puisque $r < b$, $0 < 2^r + 1 < 2^b - 1$ et donc $2^r + 1$ ne peut diviser N. Il n'y a donc finalement pas de solution au problème.

Solution de l'exercice 145 : Remarquons dans un premier temps que $1989 = 3^2 \times 13 \times 17$. Il suffit donc de prouver que la différence est un multiple de 9, de 13 et de 17.

Commençons par 13. On veut prouver que $n^a - n^b$ (avec $a = n^{n^n}$ et $b = n^n$) est un multiple de 13, c'est-à-dire que $n^a \equiv n^b \pmod{13}$. Comme pour tout x non multiple de 13, $x^{12} \equiv 1 \pmod{13}$ (d'après le petit théorème de Fermat), il suffit de prouver que $a \equiv b \pmod{12}$.

On recommence. On a $12 = 3 \times 4$, donc on doit montrer que $a \equiv b \pmod 3$ et $a \equiv b \pmod 4$. Pour 3, encore d'après le petit théorème de Fermat, il suffit de voir que n^n et n sont de même parité, ce qui est évident. Pour 4, c'est légèrement plus compliqué parce que ce n'est pas un nombre premier. On distingue deux cas : si n est pair, a et b sont des multiples de 4 et c'est fini. Sinon, on constate que pour tout entier impair x, on a $x^2 \equiv 1 \pmod 4$. L'argument précédent s'applique alors à nouveau.

On raisonne de même pour 17. Il faut comparer a et b modulo 16. Là, encore, ce n'est pas un nombre premier. Si n est pair, a et b sont des multiples de 16 (car $n \geqslant 3$). Sinon, comme pour tout x impair, on a $x^4 \equiv 1 \pmod{16}$, on est amené à comparer n et n^n modulo 4. L'égalité de ces nombres résulte du fait que n est impair.

Il ne reste plus que 9. Si n est un multiple de 3, n^a et n^b sont des multiples de 9 et donc leur différence aussi. Sinon, on est amené à comparer a et b modulo 6 (en effet, pour tout x premier à 3, on a $x^6 \equiv 1 \pmod 9$), c'est-à-dire modulo 3 et modulo 2. Et on a déjà traité ces deux cas.

Solution de l'exercice 146 : Comme M contient au moins deux éléments, il contient un nombre premier impair p. En prenant $A = \{p\}$, on obtient $2 \in M$ car il divise $p-1$.

Soit p un élément de M distinct de 2. Si $p \equiv 1 \pmod 3$, on constate comme précédemment que $3 \in M$. Si $p \equiv 2 \pmod 3$, on voit que $3 \in M$ car il divise $2p-1$. Sinon, $p = 3$ et dans tous les cas $3 \in M$.

Montrons maintenant que M est infini. On suppose par l'absurde que M est fini. Notons P le produit des éléments de M. Soit p un élément de M. Le nombre $\frac{P}{p}$ est le produit des éléments de M différents de p, donc d'après l'hypothèse sur M, le nombre $\frac{P}{p} - 1$ se décompose en produit d'éléments de M. Comme il est premier avec les éléments de M distincts de p, c'est une puissance de p. En particulier :

$$P - 2 = 2^\alpha \quad \text{et} \quad P - 3 = 3^\beta$$

pour des entiers α et β. Comme $P \geqslant 2 \times 3 \times 5 = 30$, on voit que $\alpha \geqslant 4$ et *a fortiori* $P \equiv 2 \pmod 8$. Cela entraîne $3^\beta \equiv -1 \pmod 8$, ce qui est absurde. Ainsi M est infini.

Montrons maintenant que $M = \mathcal{P}$. Soit q un nombre premier. Comme M est infini, il existe $q-1$ éléments de M ayant même résidu modulo q, forcément non nul. D'après le petit théorème de Fermat, le produit de ces nombres est congru à 1 modulo q. Si A est la partie formée par ces $q-1$ nombres, on voit directement que $q \in M$. Cela conclut.

Solution de l'exercice 147 : On remarque en premier lieu que d'après le petit théorème de Fermat 37 divise $n^{37} - n$ pour tout entier n. Le PGCD cherché est donc au moins un multiple de 37.

Cepedant, si p est un nombre premier tel que $(p-1)$ divise 36, on va avoir $36 = (p-1)\,k$ et, si n est premier avec p :

$$n^{37} - n = n\left(n^{36} - 1\right) = n\left(\left(n^{p-1}\right)^k - 1\right) \equiv 0 \pmod p$$

la dernière congruence résultant du petit théorème de Fermat. On constate que cette congruence reste vrai si n est un multiple de p. Ainsi, tout nombre premier p tel que $p-1$ divise 36 doit être du PGCD cherché. Les tels nombres premiers sont 2, 3, 5, 7, 13 et 19 et 37.

De plus, pour tout nombre premier p, on vérifie immédiatement que p^2 ne peut pas diviser $p^{37} - p$. Le PGCD est donc sans facteur carré.

Il reste à voir si les facteurs premiers trouvés précédemment sont les seuls qui apparaissent. Pour cela, on factorise $2^{37} - 2$:

$$2^{37} - 2 = 2\left(2^{36} - 1\right) = 2\left(2^{18} - 1\right)\left(2^{18} + 1\right) = 2\left(2^9 - 1\right)\left(2^9 + 1\right)\left(2^{18} + 1\right)$$

On a $2^9 - 1 = 511 = 7 \times 73$, $2^9 + 1 = 513 = 3^3 \times 19$. Dans le dernier facteur, il doit y avoir au moins les nombres premiers 5, 13 et 37, on trouve ainsi la factorisation $2^{18} + 1 = 5 \times 13 \times 37 \times 109$. Ainsi :

$$2^{37} - 2 = 2 \times 3^3 \times 5 \times 7 \times 13 \times 19 \times 37 \times 73 \times 109$$

Il ne reste donc plus qu'à tester les nombres premiers 73 et 109. On calcule pour cela 3^{37} modulo ces deux nombres. La méthode suivante est assez efficace, on calcule successivement :

$$\begin{array}{rcl} 3^2 & \equiv & 9 \pmod{109} \\ 3^4 & = & \left(3^2\right)^2 \equiv 9^2 \equiv 81 \pmod{109} \\ 3^9 & = & \left(3^4\right)^2 \times 3 \equiv 81^2 \times 3 \equiv 63 \pmod{109} \\ 3^{18} & = & \left(3^9\right)^2 \equiv 63^2 \equiv 45 \pmod{109} \\ 3^{37} & = & \left(3^18\right)^2 \times 3 \equiv (45)^2 \times 3 \equiv 80 \pmod{109} \end{array}$$

et donc $3^{37} - 3$ n'est un multiple de 109, ce qui élimine ce nombre premier. En faisant un calcul analogue, on voit (hélas !) que $3^{37} \equiv 3 \pmod{73}$, et on ne peut donc pas conclure directement. Pour éliminer 73, il faut calculer $5^{37} - 5$ modulo 73 : on trouve 63, ce qui permet d'éliminer le dernier récalcitrant.

Le PGCD cherché est finalement $2 \times 3 \times 5 \times 7 \times 13 \times 19 \times 37 = 1\,919\,190$.

Remarque. Si l'on sait que $\mathbf{Z}/p\mathbf{Z}$ est cyclique pour p premier, on peut prouver sans faire de calcul que les seuls facteurs premiers qui apparaissent dans le PGCD sont ceux que l'on a trouvés.

Solution de l'exercice 148 : Définissons la suite (u_n) par :

$$\begin{array}{rcll} u_n & = & n & \text{si } n \text{ n'est pas un multiple de 5} \\ u_n & = & 3u_{n/5} & \text{sinon} \end{array}$$

On montre par récurrence que le dernier chiffre non nul de $n!$ est congru à $u_1 \cdots u_n$ modulo 5. Pour $n = 1$, c'est évident. Supposons que ce soit le cas pour n. Remarquons que si $n + 1$ n'est pas un multiple de 5, alors le nombre de zéros terminant $n!$ sera le même que le nombre de zéros terminant $(n + 1)!$. On en déduit directement la propriété voulue dans le cas où $n + 1$ n'est pas un multiple de 5. Sinon, notons $v = v_5(n + 1)$. On peut en outre écrire $n! = 10^k r$ où r est un entier congru à $u_1 \cdots u_n$ modulo 5 et donc premier avec 5. Dans ce cas, on a :

$$(n + 1)! = 10^{k+v} \cdot \frac{n + 1}{5^v} \cdot \frac{r}{2^v}$$

On vérifie facilement que :

$$k + v + v_2\left(\frac{n + 1}{5^v} \cdot \frac{r}{2^v}\right) = v_2\left((n + 1)!\right) \geqslant v_5\left((n + 1)!\right) = k + v$$

Ainsi $\frac{n+1}{5^v} \cdot \frac{r}{2^v}$ est entier et le dernier chiffre non nul de $(n + 1)!$ est congru modulo 5 à :

$$\frac{n + 1}{5^v} \cdot \frac{r}{2^v} \equiv u_1 \cdots u_n 3^v u_{\frac{n+1}{5^v}} \equiv u_1 \cdots u_{n+1} \pmod{5}$$

comme on le veut.

Montrons que la suite (u_n) n'est pas périodique modulo 5 (même à partir d'un certain rang). Supposons que ce soit le cas et notons k une période. Supposons que k soit un multiple de 5. Dans ce cas, on a pour tout entier n (suffisamment grand), $u_{5n} = u_{5n+k}$ puis en multipliant par 3 :

$$u_n \equiv u_{n+\frac{k}{5}} \pmod 5$$

et donc $\frac{k}{5}$ est également une période. On peut donc supposer que k est premier avec 5. Pour tout entier n (suffisamment grand), on a alors :

$$u_n \equiv 2u_{5n} \equiv 2u_{5n+k} = 2\,(5n+k) \equiv 2k \pmod 5$$

ce qui est absurde.

Comme u_n est toujours premier avec 5, ce dernier résultat implique que la suite des derniers chiffres non nuls de $n!$ n'est pas périodique à partir d'un certain rang.

Solution de l'exercice 149 : Choisissons une maison et partant de celle-ci, attribuons successivement tous les entiers positifs ou nuls (dans l'ordre) aux maisons successives en tournant dans le sens des aiguilles du montre. Ainsi, la maison choisi aura le nombre 0 mais également les nombres 12, 24, *etc.* La maison qui est immédiatement après elle dans le sens des aiguilles d'une montre portera les numéros 1, 13, 25, *etc.* Si x et y sont deux nombres d'une même maison, on aura $x \equiv y \pmod{12}$.

À toute coloration des maisons, on peut associer un entier de la façon suivante. Pour toutes les maisons peintes en bleu, on regarde un nombre 2^n où n est un numéro quelconque de la maison, et on somme tous ces nombres. La somme obtenu ainsi n'est pas uniquement définie, mais par contre elle définit un résidu modulo $N = 2^{12} - 1$ (car si $x \equiv y \pmod{12}$, alors $2^x \equiv 2^y \pmod N$).

On a une propriété intéressante, conséquence directe de l'unicité de la décomposition en base 2 : si n_1 et n_2 sont des nombres associés à deux colorations, et que n_1 et n_2 définissent le même résidu modulo N (*i.e.* si $n_1 \equiv n_2 \pmod N$), alors les deux colorations sont identiques ou l'une est entièrement bleu et l'autre entièrement blanche.

Notons c_i le nombre associé à la coloration après le passage de i-ième peintre et c_0 le nombre associé à la coloration initiale. Soit i un entier compris entre 1 et 12. Si le i-ième peintre repeint les maisons $i, i+1, \ldots, i+t-2$ en blanc et la maison $i+t-1$ en bleu. On a alors :

$$c_{i+1} \equiv c_i - \left(2^i + 2^{i+1} + \cdots + 2^{i+t+2}\right) + 2^{i+t+1} = c_i - 2^{i+t+1} - 2^i + 2^{i+t+1} = c_i + 2^i \pmod N$$

On en déduit que :

$$c_{12} \equiv c_0 + 2^0 + 2^1 + \cdots + 2^{11} = c_0 + N \equiv c_0 \pmod N$$

et donc soit les colorations au début et à la fin sont identiques, soit l'une est totalement bleue, et l'autre totalement blanche.

Cependant le dernier cas ne peut pas se produire, car aucune d'entre elle ne peut être totalement blanche. En effet, par hypothèse, celle de départ ne peut pas l'être. Et celle d'arrivée non plus, car un peintre termine toujours son œuvre en repeignant une maison en bleu. Cela résout l'exercice.

Solution de l'exercice 150 : On est ramené à considérer une équation de la forme :

$$2^n = a \cdot 10^d + 2^m$$

ou a est un entier compris entre 1 et 9 et où $d+1$ désigne le nombre de chiffres de 2^n en base 10. On a $n > m$ et posons $n = m+k$ où k est un entier strictement positif. L'équation devient :

$$2^m \left(2^k - 1\right) = a10^d$$

et donc 5^d divise $2^k - 1$.

Si $d > 1$, alors il faut $2^k \equiv 1 \pmod{25}$. En regardant les puissances successives de 2 modulo 25, on voit que cela implique que k est un multiple de 20. On a alors $2^k \equiv 1 \pmod{11}$ ce qui signifie que 11 divise $2^k - 1$. Mais cela est impossible car le nombre premier 11 n'apparaît pas dans 10 et ne peut apparaître dans $a \leqslant 9$.

Reste le cas $d = 1$. Cela entraîne que 2^m a un seul chiffre et 2^n en a deux. Par une recherche exhaustive, on prouve que les seules puissances qui conviennent sont 32 et 64.

Solution de l'exercice 151 : Supposons par l'absurde que de tels entiers existent.

Soit ℓ un nombre premier. Nous allons montrer que soit ℓ divise a, soit ℓ divise b. Si ce n'était pas le cas, d'après le théorème de Dirichlet, on pourrait choisit des nombres premiers arbitrairement grands, p congru à $\frac{1}{a}$ modulo ℓ et q congru à $-\frac{1}{b}$ modulo ℓ. Alors $ap + bq \equiv 0 \pmod{\ell}$, et donc $ap + bq$ n'est pas premier (si on a choisi p et q suffisamment grands). C'est une contradiction.

On en déduit que tout nombre premier divise soit a, soit b. Mais cela est une absurdité sans nom ! Les entiers a et b n'existent donc tout simplement pas.

Autre solution. Cette autre solution, bien plus longue, a l'avantage de ne pas faire appel au théorème de Dirichlet.

Un couple (a, b) vérifiant les conditions de l'énoncé sera dit convenable. On suppose, par l'absurde, qu'il existe au moins un couple convenable, disons (a, b).

Lemme. Si (x, y) est convenable alors x et y sont distincts et premiers entre eux et tout diviseur premier de x (resp. de y) est inférieur à 1000.

Prouvons le lemme. Si $x = y$ alors, pour tous p et q premiers distincts et supérieurs à 1000 le nombre $xp + yq = x(p+q)$ est pair et supérieur à 1000. Il ne peut donc pas être premier. Donc x et y sont distincts.

Si p est un diviseur premier de x supérieur à 1000 alors pour tout q premier, distinct de p et supérieur à 1000, on a $xq + yp = k$, avec k premier et $k > p$. Or p divise k, ce qui est absurde. Donc, ni x ni y n'a de diviseur premier supérieur à 1000.

Si d est un diviseur premier commun à x et y. Alors, d'après le point précédent, on a $d < 1000$. Soient p et q deux nombres premiers distincts supérieurs à 1000. Alors d divise $xp + yq$ qui est premier et supérieur à 1000 et donc à d, ce qui est impossible. Donc x et y sont premiers entre eux.

Le lemme est donc acquis. On prouve maintenant que, si l'on définit les suites (a_n) et (b_n) par $a_0 = a$, $b_0 = b$ et, pour tout entier $n \geqslant 0$:

$$a_{n+1} = a_n^2 + b_n^2 \quad \text{et} \quad b_{n+1} = 2a_n b_n$$

alors pour tout $n \geqslant 0$, le couple (a_n, b_n) est convenable.

Bien entendu, il suffit de prouver que (a_1, b_1) est convenable, puisqu'alors une récurrence immédiate conduira impitoyablement à la conclusion désirée. Soient p et q deux nombres premiers distincts et supérieurs à 1000. On a $ap + bq = k_1$ et $aq + bp = k_2$ où k_1 et k_2 sont premiers et supérieurs à 1000. De plus, puisque $k_1 - k_2 = (a-b)(p-q)$, on déduit du lemme que $k_1 \neq k_2$. Mais alors $ak_1 + bk_2 = k_3$ avec k_3 premier, soit $(a^2+b^2)p + 2abq = k_3$. D'où $(a^2+b^2, 2ab)$ est convenable.

On note que, pour tout n, on a $a_{n+1}, b_{n+1} \geqslant 2$ et donc que $a_{n+1} > a_n$. Ceci assure entre autre que les couples (a_n, b_n) sont deux à deux distincts, et donc que l'on a ainsi construit une infinité de couples convenables.

D'autre part, pour tous $i \neq j$, les nombres a_i et a_j sont premiers entre eux. En effet, on a clairement :

$$b_j = 2^j b a_0 a_1 \cdots a_{j-1}$$

Or, d'après le lemme, on sait que a_j est premier avec b_j. Par suite a_j est premier avec tous les a_k où $k < j$.

Pour conclure, on choisit p_n un diviseur premier de a_n. D'après ce qui précède, la suite $(p_n)_{n \geqslant 1}$ est une suite infinie de nombres premiers deux à deux distincts. Mais d'après le lemme, les p_n sont tous inférieurs à 1000, ce qui est absurde.

Solution de l'exercice 152 : Pour des raisons pratiques, on commence par traiter à part les cas $n = 1$ et $n = 2$ qui sont évidents. On suppose donc à partir de maintenant que $n \geqslant 3$.

Soit p un nombre premier. Nous allons montrer que :

$$v_p(n!) \leqslant v_p\left(\prod_{k=0}^{n-1}(a^n - a^k)\right)$$

La formule de Legendre nous donne une formule pour $v_p(n!)$:

$$v_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots \leqslant \frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} + \cdots = \frac{n}{p-1}$$

On en déduit, puisque $v_p(n!)$ est un entier, que :

$$v_p(n!) \leqslant \left[\frac{n}{p-1}\right] \tag{6}$$

Réécrivons le produit dont on veut calculer la valuation sous la forme suivante :

$$P = \prod_{k=0}^{n-1}(a^n - a^k) = \prod_{k=0}^{n-1}\left(a^k\left(a^{n-k}-1\right)\right) = a^{\frac{n(n-1)}{2}} \prod_{k=0}^{n-1}\left(a^{n-k}-1\right)$$

On distingue deux cas :

- si $v_p(a) > 0$, alors le premier facteur dans l'écriture précédente prouve que $v_p(P) \geqslant \frac{n(n-1)}{2}$. Comme $n \geqslant 3$, on obtient $v_p(P) \geqslant n$ et donc d'après la majoration (6), on a bien $v_p(P) \geqslant v_p(n!)$ comme on le voulait ;

– si $v_p(a) = 0$, les entiers a et p sont premiers entre eux, et donc d'après le petit théorème de Fermat, tous les entiers k tels que $n-k$ est multiple de $p-1$ sont tels que $a^{n-k}-1$ est multiple de p, ou encore que $v_p(a^{n-k}-1) \geqslant 1$. Comme il y a $\left[\frac{n}{p-1}\right]$ tels entiers k, il vient $v_p(P) \geqslant \left[\frac{n}{p-1}\right]$ et donc la conclusion encore par la majoration (6).

<u>*Solution de l'exercice 153*</u> : On se rappelle que si $S(n)$ désigne la somme des chiffres de n, on a $S(n) \equiv n \pmod 9$. Le nombre cherché ici est donc congru à 4444^{4444} modulo 9.

Calculons donc 4444^{4444} modulo 9. Déjà il est congru à 7^{4444}. Les premières puissances de 7 modulo 9, sont :

$$7^0 \equiv 1 \pmod 9 \quad ; \quad 7^1 \equiv 7 \pmod 9 \quad ; \quad 7^2 \equiv 4 \pmod 9$$

$$7^3 \equiv 1 \pmod 9 \quad ; \quad 7^4 \equiv 7 \pmod 9$$

et la suite ainsi obtenue est périodique de période 3. Comme 4444 est congru à 1 modulo 3, on a finalement :

$$4444^{4444} \equiv 7 \pmod 9$$

Maintenant, on remarque que 4444^{4444} a $1 + 4444 \log_{10}(4444) < 16212$ chiffres. Ainsi $S(4444^{4444}) \leqslant 9 \times 16211 = 145899$. Ainsi $S \circ S(4444^{4444}) < 1 + 9 \times 5 = 46$, puis $S \circ S \circ S(4444^{4444}) < 4 + 9 = 13$.

Il ne reste plus qu'une possibilité : le nombre cherché est 7.

<u>*Solution de l'exercice 154*</u> : Notons $x = 2a+1$ et $y = 2b+1$, qui sont des entiers impairs. La condition est équivalente à 2^n divise $x^n + y^n$. Si n est pair, x^n et y^n sont congrus à 1 modulo 4 et donc la somme n'est pas un multiple de 4. On en déduit que n vaut forcément 2.

Si n est impair, on factorise :

$$x^n + y^n = (x+y)\left[x^{n-1} - x^{n-2}y + \cdots + y^{n-1}\right]$$

Le facteur entre crochets est une somme de n nombres impairs, il est donc impair. On en déduit que 2^n divise $x+y$, ce qui ne peut se produire que pour un nombre fini de n.

<u>*Solution de l'exercice 155*</u> : Commençons par prouver l'énoncé donné en indication. Soit p un diviseur premier impair de n^2+1. Ainsi on a la congruence $n^2 \equiv -1 \pmod p$ et en élevant à la puissance $\frac{p-1}{2}$, on obtient :

$$n^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod p$$

D'autre part, n est évidemment premier à p et donc d'après le petit théorème de Fermat, $n^{p-1} \equiv 1 \pmod p$. Cela implique $\frac{p-1}{2}$ pair et donc $p \equiv 1 \pmod 4$.

Nous voulons considérer un diviseur premier impair de n^2+1. Montrons que cela existe bien. Si ce n'était pas le cas, on aurait $n^2 + 1 = 2^v$ pour un certain entier v. De $n > 1$, on déduit $v \geqslant 2$ et donc $n^2 \equiv -1 \pmod 4$. Mais cette dernière congruence ne peut pas être réalisée. Un tel diviseur premier p existe donc bien et d'après ce qui précède, la fraction $k = \frac{p-1}{2}$ est un entier pair.

On en déduit directement (en utilisant $p - x \equiv -x \pmod p$) que :

$$(p-1)! \equiv (k!)^2 \pmod p$$

D'après le théorème de Wilson, ces nombres sont congrus à -1 modulo p et donc :

$$(n - k!)\,(n + k!) = n^2 - (k!)^2 \equiv 0 \pmod p$$

L'un des deux facteurs du membre de gauche est alors un multiple de $p = 2k+1$; cette remarque termine l'exercice.

Solution de l'exercice 156 : Le nombre que l'on considère :

$$\frac{(nm)!}{m!(n!)^m}$$

est le nombre de façons de partitionner l'ensemble à nm éléments $E = \{1, 2, \ldots, mn\}$ en m parties à n éléments, et c'est donc en particulier un entier. Pour le voir, on peut remarquer que chaque permutation σ de E fournit une telle partition $\{E_1, \ldots, E_m\}$ en posant :

$$E_k = \{\sigma(kn - k + 1), \ldots, \sigma(kn-1), \sigma(kn)\}$$

et bien sûr toutes les partitions sont obtenues de cette façon. En outre, si l'on permute les éléments de chacun des ensembles E_k ou que l'on permute les m ensembles E_k entre eux, on obtient la même partition. Une partition donnée correspond donc à $m!(n!)^m$ permutations distinctes de E exactement. Comme il y a $(nm)!$ permutations de E en tout, cela conclut.

Solution de l'exercice 157 : On commence par prouver que si le résultat est vrai pour n et m alors il est vrai pour nm. On considère donc $2nm-1$ entiers. D'après notre hypothèse, si l'on en choisit $2n-1$ quelconques parmi ces entiers, on peut en trouver n dont la somme s_1 est divisible par n. On écarte ces n entiers et on recommence avec les $2nm-1-n$ restants. On forme ainsi $2m-1$ groupes de n entiers, dont les sommes respectives $s_1, \cdots, s_{2m-1}$ sont toutes divisibles par n. Soit d le pgcd de m et n. Pour tout i, on pose alors $d_i = \frac{s_i}{d}$. Par hypothèse, parmi les $2m-1$ nombres d_i, on peut en trouver m dont la somme est divisible par m, disons $d_1, \cdots, d_m$. Cela assure que la somme des mn nombres entiers de départ qui appartiennent aux groupes s_i, où $i = 1, \ldots, m$, est divisible par mn, ce qui prouve bien que le résultat est vrai pour mn.

On en déduit qu'il suffit de prouver le résultat pour $n = p$ premier. Considérons dans ce cas de entiers $a_1, \cdots, a_{2p-1}$. Par l'absurde, supposons que l'on ne puisse en trouver p dont la somme soit divisible par p. Soit alors :

$$S = \sum (a_{i_1} + \cdots + a_{i_p})^{p-1}$$

où la somme porte sur toutes les parties $\{i_1, \ldots, i_p\}$ à p éléments de $\{1, 2, \cdots, 2p-1\}$. Notons qu'il y a exactement $t = \mathrm{C}_{2p-1}^{p}$ telles parties et qu'alors :

$$t = \frac{(2p-1)(2p-2)\cdots(p+1)}{(p-1)!} \not\equiv 0 \pmod p$$

D'après le petit théorème de Fermat, on a donc $S = 1 + 1 + \cdots + 1 = t \not\equiv 0 \pmod{p}$.

D'autre part, si l'on développe chaque terme $(a_{i_1} + \cdots + a_{i_p})^{p-1}$ de la somme S, on obtient une somme de termes de la forme $a_{i_1}^{e_{i_1}} \cdots a_{i_p}^{e_{i_p}}$, où les e_{i_j} sont des entiers positifs ou nuls dont la somme est égale à $p-1$. Intéressons-nous à un terme fixé de cette forme, disons $a_1^{e_1} \cdots a_r^{e_r}$, où r représente donc le nombre de a_i qui apparaîssent avec un exposant non nul. Ce terme apparaît dans S exactement autant de fois que l'on peut choisir $p-r$ termes parmi $2p-1-r$ (ceux qui ont au contraire un exposant nul dans le développement). Le coefficient de $a_1^{e_1} \cdots a_r^{e_r}$ est donc égal à :

$$\mathrm{C}_{2p-1-r}^{p-r} = \frac{(2p-1-r) \cdots p \cdots (p-r+1)}{(p-r)!} \equiv 0 \pmod{p}$$

Donc, tous les coefficients sont divisibles par p, ce qui assure que S elle-même est divisible par p. Nous avons la contradiction désirée, et le résultat demandé en découle.

<u>*Solution de l'exercice 158*</u> : On voit facilement que le k-ième enfant qui reçoit un bonbon est celui qui est numéroté $\frac{k(k+1)}{2}$ modulo n. Il s'agit donc de savoir si tout résidu modulo n peut s'écrire sous la forme $\frac{k(k+1)}{2}$.

Nous allons montrer que cela n'est vrai que si n est une puissance de 2. Soit un entier n et supposons que n admette un diviseur premier $p \geqslant 3$. Si tout résidu modulo n s'écrit sous la forme $\frac{k(k+1)}{2}$, il en est de même de tout résidu modulo p. Comme p est impair, il existe un entier d (par exemple $d = \frac{p+1}{2}$) tel que $2d \equiv 1 \pmod{p}$ et :

$$\frac{k(k+1)}{2} \equiv dk(k+1) \pmod{p}$$

Si $k \equiv 0 \pmod{p}$, la quantité précédente est nulle. Et il en est de même si $k \equiv -1 \pmod{p}$. Il est dans ces conditions impossible que toute valeur soit atteinte par cette formule. Cela est une contradiction, et donc si tout résidu modulo n est de la forme $\frac{k(k+1)}{2}$, n est forcément une puissance de 2.

Réciproquement, on procède par récurrence, en s'inspirant du lemme de Hensel, sur l'exposant de la puissance de 2. Pour $n = 2$ ou $n = 4$, on vérifie facilement à la main. Passons à l'hérédité. Donnons-nous un entier a. On cherche à construire k tel que :

$$\frac{k(k+1)}{2} \equiv a \pmod{2^m}$$

ou encore :

$$k(k+1) \equiv 2a \pmod{2^{m+1}}$$

On sait par hypothèse de récurrence, qu'il existe un entier k' tel que :

$$k'(k'+1) \equiv 2a \pmod{2^m}$$

Cherchons k sous la forme $k' + 2^m r$. On calcule :

$$k(k+1) = k^2 + k = k'^2 + 2^{m+1}k'r + 2^{2m}r^2 + k' + 2^m r \equiv k'(k'+1) + 2^m r \pmod{2^{m+1}}$$

Or, par choix de k', il existe un entier r' tel que $k'(k'+1) = 2a + 2^m r'$. Il suffit donc pour conclure de prendre $r' = -r$, ou $r' = 2t - r$ pour t suffisamment grand si l'on veut un entier k positif.

Autre solution. On indique ici une autre solution plus conceptuelle pour la seconde partie de la preuve. On a besoin pour cela de la définition et des propriétés de $\mathbf{Z}/n\mathbf{Z}$ qui sont détaillées dans la seconde partie du cours (chapitre 5). On suppose que $n = 2^m$ est une puissance de 2 et on considére l'application suivante :

$$f: \begin{array}{ccc} \mathbf{Z}/2^{m+1}\mathbf{Z} & \to & \mathbf{Z}/2^m\mathbf{Z} \\ x & \mapsto & \frac{x(x+1)}{2} \end{array}$$

Noter que l'on est obligé de choisir 2^{m+1} pour l'ensemble de départ : l'application n'est pas correctement défini si l'on prend 2^m : à cause de la division par 2, la valeur de $f(x)$ ne dépend pas que de la classe de x modulo 2^m, mais modulo 2^{m+1}.

Supposons que $f(x) = f(y)$, alors directement :

$$x(x+1) \equiv y(y+1) \pmod{2^{m+1}}$$

ce qui signifie que $(x-y)\, x+y+1$ est un multiple de 2^{m+1}. Si $x-y$ est pair, $x+y+1$ est impair, et donc on peut simplifier dans $\mathbf{Z}/2^{m+1}\mathbf{Z}$ par ce facteur. Ainsi $x = y$ dans $\mathbf{Z}/2^{m+1}\mathbf{Z}$. Si maintenant $x-y$ est impair, alors on peut simplifier par $x-y$ et on obtient $x+y+1 = 0$ dans $\mathbf{Z}/2^{m+1}\mathbf{Z}$.

Ce qui précède entraîne que tout élément de $\mathbf{Z}/2^m\mathbf{Z}$ admet au plus deux antécédents par f. Par des considérations simples de cardinalité, on voit qu'il en admet en fait exactement deux. En particulier, toutes les valeurs de $\mathbf{Z}/2^m\mathbf{Z}$ sont atteintes.

Solution de l'exercice 159 : On raisonne par récurrence sur l'entier n. On vérifie à la main pour $n \leqslant 4$. Supposons le résultat vrai pour tout $k < n$ pour un certain entier n quelconque mais néanmoins fixé. Si n est pair, c'est évident. Si n est impair, notons A (resp. B) le produit des nombres premiers inférieurs ou égaux à $\frac{n+1}{2}$ (resp. supérieurs strictement à $\frac{n+1}{2}$ et inférieurs ou égaux à n).

D'après l'hypothèse de récurrence, on a :

$$A \leqslant 4^{\frac{n+1}{2}}$$

D'autre part, chaque nombre premier apparaissant dans B divise $\mathrm{C}_n^{\frac{n+1}{2}}$ et donc B divise ce coefficient binomial et en particulier est plus petit. On en déduit :

$$AB \leqslant 4^{\frac{n+1}{2}} \mathrm{C}_n^{\frac{n+1}{2}}$$

Par ailleurs, on a :

$$2\mathrm{C}_n^{\frac{n+1}{2}} \leqslant 2 \sum_{k=\frac{n+1}{2}}^{n} \mathrm{C}_n^k = \sum_{k=0}^{n} \mathrm{C}_n^k = 2^n$$

On en déduit le résultat voulu.

Solution de l'exercice 160 : On remarque dans un premier temps que si n est impair, $2^n \equiv 2 \pmod 3$ et donc si on choisit pour $k \equiv 1 \pmod 3$, on aura $k2^n + 1 \equiv 0 \pmod 3$ qui ne pourra donc jamais être premier (du moins si $k > 1$). On a ainsi réglé le cas n impair.

Si n est pair, on aimerait trouver un nombre modulo N premier avec 3 pour faire la même manipulation. Il serait intéressant de le choisir tel que 2 soit d'ordre 2 modulo N. Seulement cela signifie que $2^2 = 4 \equiv 1 \pmod N$ et donc N divise 3. Ce n'est pas bon. On choisit donc un modulo (premier) pour lequel 2 est d'ordre 4. Ces modulos sont les diviseurs premiers de $2^4 - 1$. On choisit $p_2 = 5$ (car on ne peut pas prendre 3). Ainsi, si $n \equiv 3 \pmod 4$, on aura :

$$2^n \equiv 2^3 \pmod{p_2}$$

et puisque p_2 est un nombre premier impair, il existe un entier k_2 tel que si $k \equiv k_2 \pmod{p_2}$, on ait $k2^n+1$ multiple de p_2. Choisissant k ainsi, on règle le problème des puissances congrues à 3 modulo 4.

Mais il en reste encore. Et on ne peut plus prendre de modulo N pour lesquels 2 est d'ordre 4 (car $2^4 - 1 = 3 \times 5$ et 3 et 5 ont déjà été choisis). On cherche donc des modulos pour lesquels 2 est d'ordre 8, c'est-à-dire des diviseurs de $2^8 - 1 = 3 \times 5 \times 17$. On choisit $p_3 = 17$ et comme précédemment, on obtient un k_3 qui reglèra le cas des puissances congrues à 7 modulo 8.

On remarque quand même que :

$$2^{2^n} - 1 = F_1 F_2 \cdots F_{n-1}$$

où $F_k = 2^{2^k} + 1$ désigne le k-ième nombre de Fermat. Ainsi si F_{n-1} est premier, il restera toujours un cas qui nous échappe. Mais si F_{n-1} fait intervenir deux nouveaux facteurs premiers, on sera sauvé.

Précisément, comme précédemment on obtient des nombres premiers $p_4 = 257$, $p_5 = 65537$ et des entiers k_4 et k_5 tels que pour tout i compris entre 1 et 5 (avec $p_1 = 3$ et $k_1 = 1$), $k \equiv k_i \pmod{p_i}$ et $n \equiv -1 \pmod{2^i}$, on ait p_i divise $k2^n + 1$. Lorsque l'on arrive à p_6, on se rend compte que F_5 est composé et fait intervenir deux nouveaux facteurs premiers p_6 et p_6'. On choisit alors k_6 et k_6' de sorte que :

- pour tout $k \equiv k_6 \pmod{p_6}$ et tout $n \equiv -1 \pmod{2^6}$, on ait p_6 divise $k2^n + 1$
- pour tout $k \equiv k_6' \pmod{p_6'}$ et tout $n \equiv 2^5 - 1 \pmod{2^6}$, on ait p_6' divise $k2^n + 1$

Finalement si l'on choisit k vérifiant $k \equiv k_i \pmod{p_i}$ et $k \equiv k_6' \pmod{p_6'}$, l'entier $k2^n + 1$ sera toujours divisible soit par l'un des p_i, soit par p_6'. On peut finalement choisir k suffisamment grand pour que le nombre premier qui apparaît ne soit pas le seul facteur. Cela termine l'exercice.

Solution de l'exercice 161 : Montrons tout d'abord que n doit être une puissance de 2. En effet, supposons par l'absurde qu'un n autre qu'une puissance de 2 convienne, et soit m un entier tel que $2^n - 1$ divise $m^2 + 9$. Alors n possède un diviseur impair $\ell \geqslant 3$, et comme $2^\ell - 1$ divise $2^n - 1$, on a aussi $m^2 \equiv -9 \pmod{2^\ell - 1}$. Or $2^\ell - 1 \equiv -1 \pmod 4$, donc $2^\ell - 1$ possède un diviseur premier $p \equiv -1 \pmod 4$. Si $p \neq 3$, on a, d'après le petit théorème de Fermat :

$$1 \equiv m^{p-1} \equiv (m^2)^{(p-1)/2} \equiv (-9)^{(p-1)/2} \equiv (-1)^{(p-1)/2} 3^{p-1} \equiv -1 \pmod p$$

ce qui est absurde. Et si $p = 3$, $2^\ell \equiv (-1)^\ell \not\equiv 1 \pmod 3$, d'où encore une contradiction.

Si n est solution, il doit donc être une puissance de 2. On va voir qu'en fait, la réciproque est vraie. Soit $n = 2^k$. On a :

$$2^n - 1 = 3(2^2+1)(2^{2^2}+1)\cdots(2^{2^{k-1}}+1)$$

Or les $2^{2^\ell}+1$ pour $\ell = 0, \ldots, k-1$ sont deux à deux premiers entre eux. En effet, si $a > b$, soit d le PGCD de $2^{2^a}+1$ et $2^{2^b}+1$. Alors d est impair, et l'on a :

$$-1 \equiv 2^{2^a} \equiv \left(2^{2^b}\right)^{2^{a-b}} \equiv 1 \pmod d$$

donc $d = 1$. D'après le théorème chinois, il existe donc un entier c tel que l'on ait :

$$c \equiv 2^{2^{\ell-1}} \pmod{2^{2^\ell}+1}$$

pour $\ell = 1, \ldots, k-1$. Alors $2^\ell - 1$ divise c^2+1 pour $\ell = 1, \ldots, k-1$, et donc $2^n - 1$ divise $(3c)^2 + 9$.

Finalement, les entiers cherchés sont exactement les puissances de 2.

Solution de l'exercice 162 : Face à une telle question, il est assez naturel de penser à poser $a_i = 2pi + b_i$, où $b_i \in \{0, 1, \cdots, p-1\}$ vérifiant $b_i \equiv i^2 \pmod p$, pour $i = 1, 2, \cdots, p$. On vérifie facilement que ces nombres sont bien deux à deux distincts et que $a_p = 2p^2$ et que $0 < a_i \leqslant 2p(p-1) + p - 1 < 2p^2$ pour tout $i < p$. De plus, pour tous i et j on a :

$$\left[\frac{a_i + a_j}{2p}\right] = i + j \tag{7}$$

Soient $1 \leqslant i, j, k, l \leqslant p$ des entiers tels que $i \neq j$, $k \neq l$ et $a_i + a_j = a_k + a_l$. De (7), on déduit que $i + j = k + l$. Par suite $b_i + b_j = b_k + b_l$, c.à.d. $i^2 + j^2 \equiv k^2 + l^2 \pmod p$. Mais alors, toujours d'après (7), on a :

$$(i-k)(i+k) \equiv (l-j)(l+j) \equiv (i-k)(l+j) \pmod p \tag{8}$$

Si $i = k$ alors $j = l$. Et si $i \neq k$, alors $-(p-1) \leqslant i - k \leqslant p - 1$ avec $i - k \neq 0$, ce qui assure que $i - k$ est premier avec p. De (8), il vient alors $i + k \equiv j + l \pmod p$. En réutilisant (7), il vient alors $k = j$ et $i = l$. Ainsi, dans tous les cas, si $a_i + a_j = a_k + a_l$ c'est que $(i, j) = (k, l)$ ou $(i, j) = (l, k)$. Et donc les sommes $a_i + a_j$ pour $i < j$ sont bien deux à deux distinctes.

Solution de l'exercice 163 : Déjà, n est forcément impair. Supposons $n > 2$. Soit :

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

la décomposition en nombres premiers de n (on a alors $k \geqslant 1$). Les p_i sont impairs. On pose $p_i = 2^{a_1} b_1 + 1$ où les b_i sont des entiers impairs. On peut supposer que a_1 est le plus petit des a_i. On a alors :

$$n = (2^{a_1} b_1 + 1)^{\alpha_1} \cdots (2^{a_k} b_k + 1)^{\alpha_k}$$

On en déduit que $n \equiv 1 \pmod{2^{a_1}}$.

D'autre part, p_1 divise $2^{n-1}+1$, et donc $2^{2n-2} \equiv 1 \pmod{p_1}$. Soit g l'ordre de 2 modulo p_1, il divise $2n-2$ et d'après le petit théorème de Fermat, g divise également $p_1 - 1$. Par contre, g ne divise pas $n-1$ car sinon on aurait $2^{n-1} \equiv 1 \pmod{p_1}$ et donc $p_1 = 2$. Donc :

$$v_2(g) = 1 + v_2(n-1) \geqslant 1 + a_1 > a_1 = v_2(p_1 - 1)$$

ce qui est incompatible avec g divise $p_1 - 1$.

Finalement $n = 1$ est la seule solution.

Solution de l'exercice 164 : Soit s le nombre minimal de chiffres non nuls (en base b) d'un multiple strictement positif de $b^n - 1$. Parmi tous les multiples de $b^n - 1$ ayant s chiffres non nuls, on en choisit un, disons A, dont la somme des chiffres est minimale. Posons :

$$A = a_1 b^{n_1} + \ldots + a_s b^{n_s}$$

avec $n_1 > \cdots > n_s$. Montrons que les n_i sont deux à deux distincts modulo n. Supposons par l'absurdes qu'il existe des indices i et j distincts tels que $n_i \equiv n_j \pmod{n}$. Notons r un entier strictement supérieur à n_1 et congru modulo n à n_i et n_j. On a alors $b^r \equiv b^{n_i} \equiv b^{n_j} \pmod{b^n - 1}$ et donc le nombre :

$$B = A + (a_i + a_j) b^r - a_i b^{n_i} - a_j b^{n_j}$$

est un multiple de $b^n - 1$. Si $a_i + a_j < b$, ce nombre a $s-1$ chiffres non nuls, ce qui contredit la minimalité de s. Donc $b \leqslant a_i + a_j < 2b$. Si l'on note $a = a_1 + \cdots + a_s$ la somme des chiffres de A, celle de B vaut :

$$a - a_i - a_j + 1 + (a_i + a_j - b) = a - b + 1 < a$$

ce qui contredit la minimalité de a.

Maintenant que l'on sait que les n_i sont deux à deux distincts modulo n, on en déduit que $s \leqslant n$ (ce qui n'est pas du tout ce que l'on veut). On va montrer qu'en réalité $s = n$. Notons r_i le reste de la division euclidienne de n_i par n. Soit :

$$C = a_1 b^{r_1} + \ldots + a_s b^{r_s}$$

qui est alors un multiple non nul de $(b^n - 1)$. Puisque les r_i sont deux à deux distincts, ce qui précède est l'écriture en base b de C. On a donc un multiple de $b^n - 1$ avec pas plus de n chiffres (éventuellement nuls). La seule possibilité est donc d'avoir $C = b^n - 1$ et dans ce cas l'unicité de la décomposition en base b assure que $s = n$ (et $a_i = b - 1$ pour tout i).

Solution de l'exercice 165 : La progression arithmétique est constituée des entiers de la forme $ak + b$ pour k entier positif.

Supposons qu'il existe des entiers x et y tels que x^2 et y^3 soit de cette forme. Alors $x^6 \equiv b^3 \pmod{a}$ et $y^6 \equiv b^2 \pmod{a}$. Si y est premier avec a (ce qui équivaut à : si b premier avec a, car tout nombre premier divisant b et a divise y, et tout diviseur commun de y et a divise b), d'après Bézout il existe u tel que $uy \equiv 1 \pmod{a}$ avec $u \geqslant 0$. Alors $u^6 y^6 x^6 \equiv b^3 \pmod{a}$, soit $(ux)^6 \equiv b \pmod{a}$, et le problème est résolu... dans ce premier cas.

Mais la difficulté, c'est lorsque b et a ne sont pas premiers entre eux. Et une idée astucieuse est de construire une récurrence sur a. L'hypothèse de récurrence s'énonce ainsi : si une

progression arithmétique infinie de raison $a \leqslant n$ contient un carré et un cube, elle contient une puissance sixième. Pour $n = 1$, c'est évident. C'est presque aussi évident pour $n = 2$, puisqu'une progression arithmétique de raison 2 contient tous les nombres pairs ou tous les nombres impairs à partir d'un certain rang. Supposons que ce soit vrai pour n, et montrons que si une progression arithmétique infinie de raison $a = n+1$ contient un carré et un cube, elle contient une puissance sixième. En se limitant au cas où b et a ne sont pas premiers entre eux : appelons d leur PGCD et p un facteur premier de d, p^i étant la plus grande puissance de p divisant d. Deux cas à envisager : soit p ne divise pas $\frac{a}{d}$, soit p ne divise pas $\frac{b}{d}$, car si p divise $\frac{a}{d}$ et $\frac{b}{d}$, d n'est pas le PGCD de a et b.

Si p ne divise pas $\frac{a}{d}$, les congruences $x^2 \equiv b \pmod{a}$ et $y^3 \equiv b \pmod{a}$ entraînent, a fortiori $x^2 \equiv b \pmod{\frac{a}{p^i}}$ et $y^3 \equiv b \pmod{\frac{a}{p^i}}$. Mais $\frac{a}{p^i} \leqslant n$, donc, d'après l'hypothèse de récurrence, il existe z tel que $z^6 \equiv b \pmod{\frac{a}{p^i}}$. Et d'après le théorème chinois, il existe $t > b$ tel que :

$$\begin{array}{rcll} t & \equiv & z & \pmod{\frac{a}{p^i}} \\ t & \equiv & 0 & \pmod{p^i} \end{array}$$

puisque p^i est premier avec $\frac{a}{p^i}$. Il en résulte :

$$\begin{array}{rcccl} t^6 & \equiv & z^6 & \equiv & b \pmod{\frac{a}{p^i}} \\ t^6 & \equiv & 0 & \equiv & b \pmod{p^i} \end{array}$$

puisque b est divisible par d, donc par p^i. L'entier $(t^6 - b)$ est divisible par $\frac{a}{p^i}$ et par p^i, donc par a puisque $\frac{a}{p^i}$ est premier avec p. Donc t^6 convient.

Si p divise $\frac{a}{d}$ mais ne divise pas $\frac{b}{d}$, alors p^{i+1} divise a mais pas b, donc tous les termes $ak + b$ de la progression arithmétique sont divisibles par d donc par p^i, mais aucun n'est divisible par p^{i+1}. En particulier, la plus grande puissance de p divisant x^2 est p^i (ce qui prouve que i est pair), et la plus grande puissance de p divisant y^3 est également p^i (ce qui prouve que i est divisible par 3). L'entier i est donc multiple de 6 : $i = 6j$. Et l'on a x divisible par p^{3j} : $x^2 - b$ étant divisible par a, $\left(\frac{x}{p^{3j}}\right)^2 - \left(\frac{b}{p^{6j}}\right)$ est divisible par $\frac{a}{p^{6j}}$. De même, y est divisible par p^{2j}, et $\left(\frac{y}{p^{2j}}\right)^3$ congru à $\frac{b}{p^{6j}}$ modulo $\frac{a}{p^{6j}}$. Comme $\frac{a}{p^{6j}} \leqslant n$, l'hypothèse de récurrence s'applique : il existe z tel que z^6 congru à $\frac{b}{p^{6j}}$ modulo $\frac{a}{p^{6j}}$. Si la différence $z^6 - \frac{b}{p^{6j}}$ est divisible par $\frac{a}{p^{6j}}$, le nombre $(zp^j)^6 - b$ est divisible par a, on a donc trouvé une puissance sixième, en l'occurrence $(zp^j)^6$, dans la suite arithmétique. Ce qui achève la démonstration.

Solution de l'exercice 166 : On procède par l'absurde en supposant qu'il n'existe qu'un nombre fini de tels n. En particulier, il existe un rang N à partir duquel tous les $a(n)$ sont des puissances d'un nombre premier. On note par ailleurs $h(n) = \frac{a(n)}{b(n)}$.

On commence par remarquer que pour tout n, $b(n) > n/2$. En effet, si l'on note k le plus grand entier tel que $2^k \leqslant n$, il n'y a dans la somme $1 + 1/2 + \cdots + 1/n$ qu'un et un seul terme $1/m$ avec m divisible par 2^k, ce qui montre que $2^k > n/2$ divise $b(n)$.

Soit alors p un nombre premier impair plus grand que $N + 1$. D'après l'exercice 5.3, p divise $a(p-1)$, et donc que $a(p-1)$ est une puissance de p. Mais si l'on avait $a(p-1) = p$, il viendrait $h(p-1) < \frac{p}{(p-1)/2} = 2 + 2/(p-1) \leqslant 3$. En choisissant p assez grand[10] pour que

[10] C'est possible, puisque $h(n)$ tend vers $+\infty$ quand n tend vers $+\infty$.

$h(p-1) \geqslant 3$, on a donc nécessairement $a(p-1) > p$, et donc $a(p-1)$ est une puissance de p au moins égale à p^2.

p étant toujours choisi supérieur à $N+1$ et tel que $h(p-1) \geqslant 3$, on peut ensuite montrer par récurrence que $a(p^k-1)$ est une puissance de p au moins égale à p^2 pour tout $k \geqslant 1$. En effet, supposons le résultat pour un certain k. Alors on peut écrire :

$$\begin{aligned} h(p^{k+1}-1) &= \sum_{m=1}^{p^k-1} \frac{1}{pm} + \sum_{\substack{1 \leqslant m \leqslant p^{k+1}-1 \\ p \nmid m}} \frac{1}{m} \\ &= \frac{h(p^k-1)}{p} + \sum_{q=1}^{p^k-1} \sum_{r=1}^{p-1} \frac{1}{pq+r} \end{aligned}$$

Comme $a(p^k-1)$ est divisible par p^2 au moins, le numérateur du premier terme est divisible par p et en appliquant à nouveau le résultat de l'exercice 5.3 (en remarquant que le numérateur de la fraction $\frac{1}{pq+r} - \frac{1}{r}$ est un multiple de p, et que son dénominateur est premier à p), on trouve que p divise $a(p^{k+1}-1)$ et donc que $a(p^{k+1}-1)$ est une puissance de p. Puis, par le même argument que précédemment, la condition $h(p^{k+1}-1) \geqslant h(p-1) \geqslant 3$ assure que ce n'est pas exactement p, ce qui achève la récurrence.

Par ailleurs, pour tout $k \geqslant 2$, on a :

$$h(p^k-p) = h(p^k-1) + \sum_{r=1}^{p-1} \frac{1}{r-p^k}$$

donc $a(p^k-p)$ est aussi divisible par p.

Choisissons alors un entier n tel que p^n ne divise pas le numérateur de $1+1/2+\cdots+1/(p-1)$, et un entier $k > n$ tel que $p^k-p > 2p^n$. Alors $a(p^k-p)$ est une puissance de p telle que $a(p^k-p) \geqslant b(p^k-p) \geqslant (p^k-p)/2 \geqslant p^n$, donc p^n divise $a(p^k-p)$, et aussi $a(p^k-1)$ pour la même raison. Donc il divise le numérateur de la différence $h(p^k-p)-h(p^k-1)$, c'est-à-dire de :

$$\frac{1}{1-p^k} + \frac{1}{2-p^k} + \cdots + \frac{1}{p-1-p^k}$$

Mais le numérateur de cette fraction est congru modulo p^k à celui de la fraction :

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$

mais p^n ne divise pas ce numérateur par définition de n. C'est une contradiction et le résultat s'ensuit.

5.4 Exercices de « *Équations diophantiennes* »

Solution de l'exercice 167 : **a)** Supposons que $n\,(n+1)$ soit un carré parfait. Comme n et $n+1$ sont premiers entre eux, ils doivent être tous les deux des carrés parfaits Mais ceci n'est pas possible pour des carrés non nuls.

Remarque. La même démonstration s'applique pour prouver que le produit de deux entiers consécutifs n'est jamais une puissance parfaite.

b) Supposons que $(n-1)\,n\,(n+1)$ soit un carré parfait. Comme n et $(n-1)\,(n+1) = n^2-1$ sont premiers entre eux, ils doivent être tous les deux des carrés parfaits. Mais pour n^2-1 soit un carré parfait, il faut $n = \pm 1$ et alors le produit $(n-1)\,n\,(n+1)$ est nul.

c) L'expression $(n-1)\,n\,(n+1)\,(n+2)$ est de degré 4 et donc sa racine carrée doit être proche d'une expression de degré 2. Plus précisément, on vérifie que l'on a la formule :

$$(n-1)\,n\,(n+1)\,(n+2) = \left(n^2+n-1\right)^2 - 1$$

On obtient à nouveau deux carrés qui diffèrent de 1 ; à nouveau la seule possibilité est que le produit soit nul.

Solution de l'exercice 168 : On applique pas à pas la méthode du cours. On commence par remarquer que $x = 1$, $y = 0$ est une solution évidente. On introduit donc un rationnel t tel que $y = t\,(x-1)$. L'équation devient :

$$x^2 + 3t^2\,(x-1)^2 = 1$$

Les solutions sont $x = 1$ et $x = \frac{3t^2-1}{3t^2+1}$. Le y correspondant vaut $y = -\frac{2t}{3t^2+1}$.

Finalement, les solutions sont les couples :

$$\left(\frac{3t^2-1}{3t^2+1}, -\frac{2t}{3t^2+1}\right)$$

pour t décrivant l'ensemble des nombres rationnels et le couple $(1, 0)$.

Solution de l'exercice 169 : **a)** La condition implique que a doit être une puissance de 5, donc $a = 5^k$. L'équation se réécrit alors $2k = n$, ce qui implique que n doit être pair. Ainsi il y a une solution pour tout entier n pair, le a correspondant étant $a = 2^{n/2}$.

b) On peut factoriser l'expression fournit et obtenir :

$$5^n = (a-1)\,(a+1)$$

Ainsi les deux nombres $a-1$ et $a+1$ doivent être des puissances cinquièmes. Or il n'existe pas deux puissances cinquièmes qui diffèrent de 2. L'équation n'a pas de solution.

c) En regardant modulo 4, on obtient $a^2 \equiv 3 \pmod 4$ puisque $5 \equiv 1 \pmod 4$. Or on sait qu'un carré modulo 4 ne peut être congru qu'à 0 ou 1. L'équation n'a donc pas de solution non plus.

Solution de l'exercice 170 : Quitte à multiplier tous les x_i par un même facteur, on peut supposer que tous les x_i sont entiers. Quitte à permuter les x_i, on peut supposer que x_1 est le plus petit d'entre eux. Posons $y_i = x_i - x_1 \geqslant 0$. On a $y_1 = 0$ et la famille des y_i vérifient la même hypothèse que la famille des x_i.

Soit $2 \leqslant i \leqslant 2002$ un entier. Notons I un sous-ensemble de $\{2, \ldots, 2002\}$ de cardinal 7 contenant i et I' l'ensemble I obtenu en remplaçant i par 1. Par hypothèse, il existe des ensembles J et J' de cardinal 11 tels que :

$$11 \sum_{i \in I} y_i = 7 \sum_{j \in J} y_j \quad \text{et} \quad 11 \sum_{i \in I'} y_i = 7 \sum_{j \in J'} y_j$$

En soustrayant ces deux égalités, on voit que $11 y_i$ est un multiple de 7 et donc d'après le lemme de Gauss qu'il en est de même de y_i. Ceci est vrai pour tout i.

La famille constitué des $\frac{y_i}{7}$ est encore solution du problème. Le principe de descente infinie assure que l'unique solution est alors $y_i = 0$ pour tout i. Cela entraîne bien que tous les x_i sont égaux.

Solution de l'exercice 171 : On trouve en premier lieu une solution particulière : $x_0 = \frac{3}{5}$, $y_0 = \frac{4}{5}$ et $z_0 = \frac{6}{5}$.

Comme un dénominateur commun de x_0^3, y_0^3 et z_0^3 est 125, si on multiplie x_0^3, y_0^3 et z_0^3 par un nombre congru à 1 modulo 125, on ne changera pas la partie décimale. On cherche donc des cubes congrus à 1 modulo 125. Les nombres de la forme $(125k + 1)^3$ s'imposent.

On est finalement amené à considérer les nombres :

$$x = x_0 (125k + 1) \quad ; \quad y = y_0 (125k + 1) \quad ; \quad z = z_0 (125k + 1)$$

dont il est facile de vérifier qu'ils conviennent.

Solution de l'exercice 172 : Soit $x = 12^m - 5^n$ le minimum cherché. On a $x \equiv -5^n \pmod 6$, donc x n'est divisible ni par 2, ni par 3. De même x n'est pas divisible par 5. Par conséquent, on a $x = 1$ ou $x \geqslant 7 = 12 - 5$. Il reste donc à exclure le cas $x = 1$. Pour cela, on peut remarquer que :

$$12^m - 5^n \equiv -1 \not\equiv 1 \pmod 4$$

Finalement, on a $x = 7$.

Solution de l'exercice 173 : La somme de tous les carrés modulo 9 vaut $\frac{9 \cdot (9+1)(18+1)}{6} \equiv 3 \cdot 5 \cdot 1 \equiv 6 \pmod 9$. La somme des carrés de 99 entiers consécutifs $x+1$, $x+2$, ..., $x+99$ vaut donc $11 \times 6 \equiv 3 \pmod 9$. En particulier, la valuation 3-adique de cette somme est exactement 1, et ce n'est donc jamais une puissance parfaite.

L'équation proposée dans l'énoncé n'a donc aucune solution.

Solution de l'exercice 174 : Nous partons de la formule :

$$(t+1)^3 + (t-1)^3 + (-t)^3 + (-t)^3 = 6t$$

qui prouve déjà que tout multiple de 6 peut s'écrire comme somme de quatre cubes. Soit n un entier. On veut réussir à écrire n (d'une infinité de façon) comme somme de cinq cubes. Mais, d'après ce qui précède, chaque fois que l'on arrive à trouver un cube congru à $-n$ modulo 6, on obtient une telle écriture. En effet, si l'on a $n = x^3 + 6t$ pour des entiers t et x, on aura de fait :

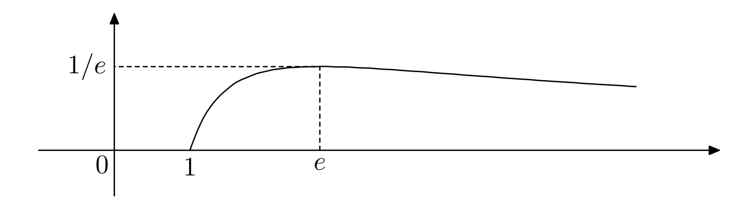
$$n = x^3 + (t+1)^3 + (t-1)^3 + (-t)^3 + (-t)^3$$

Or on vérifie facilement que tout résidu modulo 6 est un cube (en réalité, on a $a^3 \equiv a \pmod 6$ pour tout a). On obtient donc bien une infinité de x qui fournissent, par le fait, une infinité de solutions.

Solution de l'exercice 175 : En prenant le logarithme, l'équation s'écrit aussi $y \log x = x \log y$, soit encore :

$$\frac{\log x}{x} = \frac{\log y}{y}$$

Une étude de fonction montre que la fonction $t \mapsto \frac{\log t}{t}$ est croissante sur l'intervalle $[1, e]$ et décroissante sur l'intervalle $[e, +\infty[$. Plus visuellement, la résentation graphique de la fonction est :



En particulier, si x et y sont deux entiers distincts (disons $x < y$) tels que $x^y = y^x$, on doit avoir $x < e$, et donc $x = 2$, ce qui conduit à $y = 4$.

Finalement les solutions sont les couples (x, y) avec $x = y$ et les deux couples $(2, 4)$ et $(4, 2)$.

Solution de l'exercice 176 : Pour commencer, comme $2^2 + 3^2 = 13$ n'est pas une puissance parfaite, on peut supposer p impair. On a alors la factorisation :

$$2^p + 3^p = 5(2^{p-1} - 3 \cdot 2^{p-2} + \cdots + 3^{p-1})$$

En particulier, 5 divise $2^p + 3^p = a^n$, donc 25 aussi. Mais $3 \equiv -2 \pmod 5$, donc on a :

$$0 \equiv 2^p + 3^p = 5 \cdot p 2^{p-1} \pmod{25}$$

Cela impose que 5 divise p, c'est-à-dire que $p = 5$. Mais $2^5 + 3^5 = 275 = 5^2 \cdot 11$ n'est pas une puissance parfaite.

On a bien montré que $2^p + 3^p$ n'était une puissance parfaite non triviale pour aucun nombre premier p.

Solution de l'exercice 177 : Notons $a_n = 1 + 2! + \cdots + n!$. On peut remarquer que pour tout entier n et tout $n \geqslant N - 1$, on a $a_n \equiv a_{N-1} \pmod{N!}$. Ainsi, pour tout $n \geqslant 2$, a_n est divisible par 3. Si par chance a_n n'était pas divisible par 9 pour n assez grand, on obtiendrait immédiatement que a_n n'est pas une puissance parfaite. Malheureusement $a_5 = 153$ est divisible par 9. Mais si l'on poursuit courageusement les calculs jusqu'à a_8, on trouve que :

$$a_8 = 46233 \equiv 9 \pmod{27}$$

Cela signifie que si pour $n \geqslant 8$, a_n est une puissance parfaite, alors ça doit être un carré parfait, puisque sa valuation 3-adique est 2.

D'autre part, on peut remarquer que $a_4 = 33 \equiv 3 \pmod 5$ n'est pas un carré modulo 5. Il en résulte avec ce qui précède que l'équation n'a pas de solution pour $n \geqslant 8$.

On peut examiner les cas restants à la main. On a :

$$\begin{array}{lcll} a_1 & = & 1 & \text{qui est une puissance } k\text{-ième pour tout } k. \\ a_2 & = & 3 & \text{qui n'est pas une puissance parfaite.} \\ a_3 & = & 9 & \text{qui est un carré parfait.} \\ a_4 & = & 33 & \text{qui n'est pas une puissance parfaite.} \\ a_5 & = & 153 = 9 \cdot 17 & \text{qui n'est pas une puissance parfaite.} \\ a_6 & = & 873 = 9 \cdot 97 & \text{qui n'est pas une puissance parfaite.} \\ a_7 & = & 5913 = 81 \cdot 73 & \text{qui n'est pas une puissance parfaite.} \end{array}$$

donc les triplets (m, n, k) solutions sont $(1, 1, k)$ pour tout $k \geqslant 2$ et $(3, 3, 2)$.

Solution de l'exercice 178 : Soit (x, y) une éventuelle solution de l'équation $y^2 = x^3 + 16$, qui s'écrit encore $(y - 4)(y + 4) = x^3$. Si y est impair, $y - 4$ et $y + 4$ sont premiers entre eux, et sont donc deux cubes impairs distants de 8, ce qui n'existe pas. Donc $y = 2y'$ est pair, et par suite $x = 2x'$ aussi. L'équation devient donc :

$$(y' + 2)(y' - 2) = 2(x')^3$$

En réduction modulo 4, il vient donc $(y' + 2)^2 \equiv 0 \text{ ou } 2 \pmod 4$, et donc forcément $(y' + 2)^2$ est divisible par 4, et ainsi y' est pair. Donc on peut encore réécrire $y' = 2s$, $x' = 2t$, et il vient $(s + 1)(s - 1) = 4t^3$. Mais alors $s + 1$ et $s - 1$ sont pairs, donc $s = 2u + 1$ est impair, et l'on obtient finalement :

$$u(u + 1) = t^3$$

Cela impose que u et $u + 1$, qui sont premiers entre eux, soient tous les deux des cubes, et donc $u = -1$ ou 0 et $t = 0$.

En remontant, on trouve que l'équation initiale possède exactement deux solutions entières, qui sont $(x, y) = (0, \pm 4)$.

Solution de l'exercice 179 : L'examen des premiers cas suggère que les couples de nombres de Fibonacci consécutifs sont solutions : $(1, 2)$, $(2, 3)$, $(3, 5)$, $(5, 8)$, etc. et il est facile de le vérifier de manière générale. En effet, si (m, n) convient, alors :

$$(m + n)^2 - n(m + n) - n^2 = m^2 + 2mn + n^2 - mn - 2n^2 = -(n^2 - mn - m^2)$$

et donc $(n, m + n)$ convient aussi. En calculant les termes de la suite de Fibonacci inférieurs à 1981 :

$$1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597$$

on obtient que $m^2 + n^2$ peut atteindre $1597^2 + 987^2$. On aimerait que cette valeur soit effectivement le maximum.

Pour le voir, il suffit d'effectuer l'opération $(m, n) \mapsto (n, m + n)$ dans l'autre sens ! En effet, soit (m, n) une solution avec $1 \leqslant m < n$, alors $(n - m, m)$ aussi. En itérant ce procédé, on se ramène nécessairement à une solution de la forme $(1, n)$. Or pour $m = 1$ l'éqution devient :

$$n^2 - n = 0 \text{ ou } 2$$

dont la seule solution strictement positive est $n = 2$. Il en résulte que toutes les solutions sont obtenues à partir de $(1, 2)$ par itération de $(m, n) \mapsto (n, m+n)$, donc sont toutes de la forme (F_{n-1}, F_n).

Finalement, le maximum possible de $m^2 + n^2$ est exactement $1597^2 + 987^2$.

Solution de l'exercice 180 : Quitte à soustraire une masse commune à toutes les vaches, on peut supposer que l'une d'entre elles a une masse nulle. Il s'agit alors de montrer qu'elles ont toutes une masse nulle.

Pour cela, soit M la somme des masses de toutes les vaches du troupeau. On sait que la masse m d'une vache quelconque est telle que $M - m$ soit pair, puisque c'est la somme des masses de deux groupes de vaches de même masse totale. Il en résulte que les masses de toutes les vaches sont de la parité de M. Comme l'une des vaches a une masse nulle, toutes les vaches ont une masse paire. Mais alors un troupeau composé de vaches de masses moitié vérifie encore les hypothèses de l'énoncé, et donc toutes les masses moitié sont encore paires. La descente infinie qui s'amorce ainsi montre clairement que toutes les masses sont nécessairement nulles.

Solution de l'exercice 181 : Déjà, si $z = 1$, on a forcément $x = y = 1$. Supposons donc $z \geqslant 2$. Si on n'a pas $x = y = z$, au moins un des deux nombres parmi x et y doit être strictement plus grand que z, et donc plus grand ou égal à $z + 1$.

Si c'est x, on obtient :

$$2x^x \geqslant 2\left(z+1\right)^{z+1} > 2z^{z+1} \geqslant 4z^z$$

ce qui est absurde.

Si c'est y, on écrit :

$$y^y \geqslant \left(z+1\right)^{z+1} > z^{z+1} + \left(z+1\right)z^z = \left(2z+1\right)z^z \geqslant 5z^z$$

ce qui est tout aussi absurde.

Solution de l'exercice 182 : On remarque que $x = 1$, $y = -a$ est toujours solution de l'équation.

D'autre part, si (x, y) est une solution de l'équation, x est racine du polynôme :

$$X^2 + ayX + \left(y^2 - 1\right) = 0$$

et l'autre racine de ce polynôme est donc $-ay - x$. On obtient ainsi une nouvelle solution qui est le couple $(-ay - x, y)$. De même, on a la solution $(x, -ax - y)$.

D'autre part, si $|a| > 2$, et si x et y sont non nuls, on a :

$$\min\left(\left|-ay-x\right|, \left|y\right|\right) > \min\left(\left|x\right|, \left|y\right|\right) \quad \text{ou} \quad \min\left(\left|x\right|, \left|-ax-y\right|\right) > \min\left(\left|x\right|, \left|y\right|\right)$$

Supposons dans un premier temps $|x| \leqslant |y|$, alors :

$$\left|-ay-x\right| = \left|ay+x\right| \geqslant \left|ay\right| - \left|x\right| \geqslant \left|a\right|\left|y\right| - \left|x\right| \geqslant \left(\left|a\right|-1\right)\left|y\right| > \left|y\right| \geqslant \min\left(\left|x\right|, \left|y\right|\right)$$

De même, si $|y| \leqslant |x|$, on a :

$$\left|-ax-y\right| > \left|x\right| \geqslant \min\left(\left|x\right|, \left|y\right|\right)$$

Posons alors $x_0 = 1$ et $y_0 = -a$. Grâce à ce qui a été fait précédemment, on construit une suite de solutions (x_n, y_n) telles que :

$$\min\left(|x_{n+1}|, |y_{n+1}|\right) > \min\left(|x_n|, |y_n|\right)$$

Cette dernière condition assure que toutes les solutions sont deux à deux distinctes. L'équation admet donc dans ce cas une infinité de solutions.

Si $a = 2$, l'équation se réécrit $(x - y)^2 = 1$ qui admet également une infinité de solutions. De même si $a = -2$, il y a une infinité de solutions. Si $a = 1$, l'équation fournit $x^2+y^2 = 1-xy$ et $(x + y)^2 = 1 + xy$. Les nombres $1 - xy$ et $1 + xy$ doivent donc être positifs et cela ne peut se produire pour une infinité de couples d'entiers (x, y). On raisonne de même si $a = -1$. Finalement pour $a = 0$, l'équation n'admet clairement qu'un nombre fini de solutions.

La réponse à la question de l'énoncé est finalement l'ensemble des entiers a tels que $|a| \geqslant 2$.

Remarque. L'équation se réécrit sous la forme :

$$\left(x + \frac{a}{2}y\right)^2 + \left(1 - \frac{a^2}{4}\right)y^2 = 1$$

On voit directement sous cette écriture que si $a^2 < 4$, l'équation ne peut admettre qu'un nombre fini de solutions. En outre, on reconnaît (du moins lorsque a est pair) une équation de Pell-Fermat. Le résultat est donc une conséquence de la résolution de cette équation. Notez cependant que l'existence d'une solution non triviale à cette équation n'est pas une évidence (et n'a pas été traité dans le cours pour l'instant). Cependant, ici, on dispose de cette solution non triviale donnée par $x = 1$ et $y = -a$.

Solution de l'exercice 183 : Pour $A \leqslant 2$, on a :

$$Axy \leqslant x^2 + y^2 < x^2 + y^2 + 1$$

donc l'équation $x^2 + y^2 + 1 = Axy$ n'a pas de solution entière. Il s'agit donc de montrer qu'elle n'en a pas non plus pour $A \geqslant 4$.

En effet, soit (x_0, y_0) une telle solution. Alors en considérant le second point d'intersection de la conique avec la droite horizontale (resp. verticale) passant par (x_0, y_0), on voit que $(x_0, Ax_0 - y_0)$ (resp. $(Ay_0 - x_0, y_0)$) est encore solution. On peut donc, par descente infinie, construire une solution (x, y) vérifiant $x \leqslant Ay - x$ et $y \leqslant Ax - y$. Il vient alors :

$$x^2 + y^2 + 1 = Ax \cdot y \geqslant 2y^2 \quad \text{et} \quad x^2 + y^2 + 1 = Ay \cdot x \geqslant 2x^2$$

Ainsi, on obtient $|x^2 - y^2| \leqslant 1$, ce qui impose $x = y$ ou $(x, y) = (1, 0)$ ou $(0, 1)$. On vérifie aisément que ces différents cas ne fournissent pas de solution à l'équation.

Finalement, on a bien montré que si $\frac{x^2+y^2+1}{xy}$ est un entier, alors c'est 3.

Solution de l'exercice 184 : Soit (x, y, z) une éventuelle solution non nulle à l'équation $x^2 + y^2 = 7z^2$. Si 7 divise x ou y, alors clairement 7 divise x et y, et donc $x^2 + y^2$ est divisible par 7^2 et finalement 7 divise z. Par conséquent $(x/7, y/7, z/7)$ est encore une solution entière

non nulle, et une descente infinie permet donc d'obtenir une solution (x, y, z) avec x et y premiers à 7. Mais il vient alors :

$$x^2 + y^2 \equiv 0 \pmod 7 \quad \text{donc} \quad (xy')^2 \equiv -1 \pmod 7$$

où y' est l'inverse de y modulo 7. Mais l'on vérifie facilement que -1 n'est pas un carré modulo 7.

Finalement, la seule solution de l'équation $x^2 + y^2 = 7z^2$ est la solution nulle $(x, y, z) = (0, 0, 0)$.

Solution de l'exercice 185 : Soit $(a, b, c) \neq (0, 0, 0)$ une éventuelle solution de l'équation :

$$a^4 + (a + b)^4 + b^4 = c^2$$

Si a et b sont pairs, alors 2^4 divise le membre de gauche, donc aussi c^2, et c est multiple de 4. Alors $(a/2, b/2, c/4)$ est encore solution. Une descente infinie permet alors de supposer que a ou b est impair.

Si exactement l'un des deux nombres a et b, par exemple a, est pair, on remarque alors que :

$$a^4 + (a + b)^4 + b^4 \equiv 0 + 1 + 1 \equiv 2 \pmod 4$$

ce qui ne saurait être un carré. Par conséquent, on doit avoir a et b impair, mais alors :

$$a^4 + (a + b)^4 + b^4 \equiv 1 + 0 + 1 \equiv 2 \pmod 4$$

fournit une nouvelle contradiction.

Finalement, le seul couple (a, b) tel que $a^4 + (a + b)^4 + b^4$ soit un carré est $(0, 0)$.

Solution de l'exercice 186 : **a)** On peut supposer $a \leqslant b \leqslant c$. On obtient $\frac{1}{4} \leqslant \frac{3}{a^2}$ et donc $a^2 \leqslant 12$. Ainsi $a = 1$, $a = 2$ ou $a = 3$. On ne peut évidemment ni avoir $a = 1$, ni $a = 2$.

Si $a = 3$, l'équation devient :

$$\frac{1}{b^2} + \frac{1}{c^2} = \frac{1}{4} - \frac{1}{9} = \frac{5}{36}$$

Comme précédemment, on montre que $b^2 \leqslant \frac{72}{5}$ puis $b = 3$. Il vient alors $c = 6$.

Les solutions sont donc les triplets $(3, 3, 6)$, $(3, 6, 3)$ et $(6, 3, 3)$

b) Comme précédemment, on montre que ni $n = 2$, ni $n = 3$ ne conviennent. Pour $n = 4$, il suffit de prendre $x_1 = x_2 = x_3 = x_4 = 2$.

On remarque que si $(x_1, \ldots, x_n)$ convient alors $(2x_1, 2x_1, 2x_1, 2x_1, x_2, x_3, \ldots, x_n)$ convient également, ce qui montre que si n est solution alors $n + 3$ l'est aussi.

D'autre part, la solution du a) fournit $(2, 2, 2, 3, 3, 6)$, qui fournit ensuite $(2, 2, 2, 3, 3, 9, 9, 18)$. Ainsi $n = 6$ et $n = 8$ sont solutions. Par suite, tous les entiers autres que 2, 3 et peut-être 5 sont solutions.

Reste à prouver que $n = 5$ n'est pas une solution. Si (a, b, c, d, e) convenait, avec $a \leqslant b \leqslant c \leqslant d \leqslant e$, alors comme précédemment, on déduirait que $1 < a^2 \leqslant 5$ et donc $a = 2$. On réinjecte, et il vient successivement par les mêmes arguments $b = 2$, $c = 2$, $d = 2$ et donc $\frac{1}{e^2} = 0$, ce qui est absurde.

Solution de l'exercice 187 : On remarque que pour $x \neq 0$ on a l'encadrement :

$$\left(x^2 + \frac{x}{2}\right)^2 < 1 + x + x^2 + x^3 + x^4 < \left(x^2 + \frac{x}{2} + 1\right)^2$$

Si x est pair, le membre central est compris entre deux carrés consécutifs et donc ne peut pas être un carré. Si x est impair, le seul entier compris entre $x^2 + \frac{x}{2}$ et $x^2 + \frac{x}{2} + 1$ est $x^2 + \frac{x}{2} + \frac{1}{2}$ et donc on doit forcément avoir :

$$\left(x^2 + \frac{x}{2} + \frac{1}{2}\right)^2 = 1 + x + x^2 + x^3 + x^4$$

ce qui conduit à $x^2 - 2x - 3 = 0$ qui admet pour solution $x = 1$ et $x = -3$.

Finalement les solutions sont $x = 0$, $x = 1$ et $x = -3$.

Solution de l'exercice 188 : Soit (a, b, c, d) des entiers non nuls vérifiant :

$$a^2 + 5b^2 = 2c^2 + 2cd + 3d^2 = 2\left(c + \frac{d}{2}\right)^2 + \frac{5}{2}d^2$$

soit, en multipliant par 4 :

$$4a^2 + 20b^2 = 2\left(2c + d\right)^2 + 10d^2$$

Modulo 5, cette équation devient :

$$4a^2 \equiv 2\left(2c + d\right)^2 \pmod 5$$

Comme les carrés modulo 5 sont 0, 1 et -1, cela impose nécessairement que a et $2c + d$ soient divisibles par 5. Or :

$$4a^2 - 2\left(2c + d\right)^2 = 10d^2 - 20b^2$$

Le premier membre étant divisible par 25, il en est de même du second et donc on obtient que $d^2 \equiv 2b^2 \pmod 5$, ce qui impose encore que 5 divise b et d. Par conséquent, 5 divise a, b, c, d, et $(a/5, b/5, c/5, d/5)$ fournit une nouvelle solution entière.

Une descente infinie permet alors immédiatement de conclure qu'il n'y a pas de solution non nulle à l'équation.

Solution de l'exercice 189 : Pour des raisons de parité, l'un des deux nombres p ou q vaut 2. Par symétrie des rôles, on suppose $q = 2$. Par suite, p est un nombre premier impair tel que :

$$p^r \pm 1 = 2^s$$

Si r est impair, $p^r \pm 1$ est un multiple de :

$$p^{r-1} \pm p^{r-2} + p^{r-3} \pm \cdots \pm p + 1$$

qui est un nombre impair strictement supérieur à 1. Il ne peut donc pas diviser 2^s. On en déduit que r est pair.

Posons $r = 2t$. Le nombre p^{2t} est alors un carré impair qui est donc congru à 1 modulo 4. Ainsi $p^r + 1 \equiv 2 \pmod 4$ et donc $p^r + 1 = 2^s$ entraîne $s = 1$, ce qui est exclus.

Il reste à étudier $p^{2t} - 1 = 2^s$. Le produit $(p^t - 1)(p^t + 1)$ est une puissance de 2 et donc il en est de même de chacun des facteurs. Deux puissances de 2 qui diffèrent de 2 ne peuvent être que 2 et 4. Ceci entraine $p = 3$ et $t = 1$, donc $r = 2$.

Les deux seules solutions sont $p = 3$, $q = 2$, $r = 2$, $s = 3$ et $p = 2$, $q = 3$, $r = 3$, $s = 2$.

Solution de l'exercice 190 : On remarque d'abord que :

$$2002^{2002} = 2002^{2001} \cdot 2002 = (2002^{667})^3 \cdot (10^3 + 10^3 + 1^3 + 1^3)$$

donc 2002^{2002} s'écrit comme somme de quatre cubes. On va voir que cette valeur est optimale.

La présence de cubes nous invite à examiner l'équation modulo une puissance de 3. Modulo 9, on a déjà :

$$2002^{2002} \equiv 4^{2002} \equiv 4^{6 \cdot 333 + 4} \equiv 4^4 \equiv 4 \pmod 9$$

car $\varphi(9) = 6$. Or les cubes modulo 9 sont 0, 1 et -1, ce dont on déduit aussitôt que 4 n'est pas somme de trois cubes ou moins.

Le résultat est donc $t = 4$.

Solution de l'exercice 191 : On remarque que l'équation se factorise sous la forme :

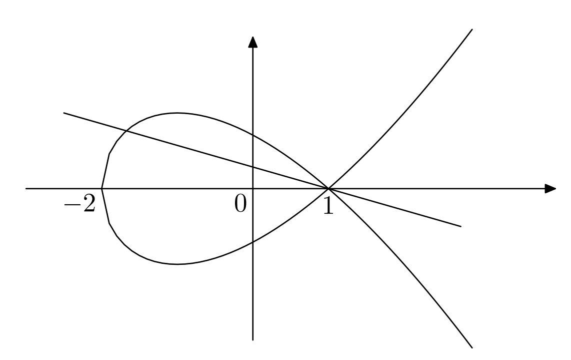
$$y^2 = (x-1)^2 (x+2)$$

Si (x, y) est une solution, posons $t = \frac{y}{x-1}$. On obtient alors : $x = 2 - t^2$ et donc t est entier. Cela donne directement toutes les solutions qui sont :

$$\left(2 - t^2, t\left(1 - t^2\right)\right)$$

pour t décrivant $\mathbf{Z}$.

Remarque. Voici l'allure de la courbe d'équation $y^2 = x^3 - 3x + 2$.



Ce n'est pas une courbe elliptique. On remarque que le point $(1, 0)$ joue un rôle particulier (il n'y a pas clairement *une* tangente en ce point). On dit que l'on a affaire à un point singulier. L'existence d'un tel point permet d'appliquer la méthode des équations de degré 2 pour décrire tous les autres points de la courbe à coordonnées rationnelles : on trace une droite passant par ce point et on cherche les autres intersections de cette droite avec la

courbe. Le fait que le point soit singulier implique en réalité que l'on va avoir une racine double alors de la résolution de l'équation qui va apparaître, et donc un unique autre point d'intersection, forcément rationnel.

La rédaction donnée ci-dessus correspond exactement à l'application de cette méthode : le paramètre t correspond à la pente de la droite tracée.

Solution de l'exercice 192 : On commence par chercher une petite solution à l'équation. On peut par exemple remarquer que :

$$1^2 + 2^2 + 3^2 + 4^2 + 5^2 = 55 = 120 - 65 = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 - 65$$

Il s'agit ensuite, à partir d'une solution (x, y, z, u, v), avec au moins quatre des cinq entiers supérieurs à 2, de trouver une autre solution plus grande. On considère alors le plus petit entier (ou l'un des plus petits) parmi x, y, z, u, v, disons x, et l'on regarde l'équation :

$$x^2 + y^2 + z^2 + u^2 + v^2 = xyzuv - 65$$

comme une équation du second degré en x. On obtient immédiatement que $(yzuv-x, y, z, u, v)$ fournit une autre solution, et l'on a $yzuv \geqslant 8y > x$, donc c'est bien une solution « plus grande ».

Plus précisément, le minimum des quatre nombres ne diminue pas quand on applique ce procédé, et il augmente strictement au bout d'au plus cinq étapes (dans le cas hypothétique où l'on serait parti d'une solution avec $x = y = z = u = v$). On finit donc bien par aboutir, après un certain nombre d'itérations, à une solution avec x y, z, u et v tous supérieurs à 1998.

En fait, six itérations suffisent, et l'on obtient alors la solution suivante, qui convient, et que l'on ne recopie que pour l'amusement du lecteur :

$$\begin{aligned} x &= 7138 \\ y &= 16\,988\,437 \\ z &= 72\,151\,760\,667\,066 \\ u &= 1\,041\,175\,313\,471\,572\,184\,867\,943\,319 \\ v &= 9\,109\,630\,532\,627\,114\,315\,851\,511\,163\,018\,235\,051\,842\,553\,960\,810\,405 \end{aligned}$$

Solution de l'exercice 193 : La relation $x^n + 1 = y^{n+1}$ s'écrit encore :

$$x^n = (y-1)(1 + y + \cdots + y^n) \tag{9}$$

Dès lors, si p est un diviseur premier de $y - 1$, p divise x, et donc ne divise pas $n + 1$, qui est premier avec x. Mais on a :

$$1 + y + \cdots + y^n \equiv n + 1 \pmod{y-1}$$

et par conséquent p ne divise pas non plus $1+y+\cdots+y^n$. Ainsi, $y-1$ et $1+y+\cdots+y^n$ sont premiers entre eux. Il en résulte, d'après (9), que $1 + y + \cdots + y^n$ est une puissance n-ième. Mais c'est impossible, puisque c'est un entier strictement compris entre les deux puissances n-ièmes consécutives y^n et $(y + 1)^n$: il n'y a donc pas de solution.

Solution de l'exercice 194 : Posons $x = \frac{a}{b^2}$ et montrons que x est entier.

Si $a \geqslant b$, alors $a^{b^2} = b^a \leqslant a^a$ et donc $a \geqslant b^2$. Donc $a^{2b^2} = b^{2a} \leqslant a^a$ et donc $a \geqslant 2b^2$. Par suite :

$$x^{b^2} = b^{a-2b^2}$$

est entier. On en déduit que x est entier (puisqu'il est rationnel). L'équation devient :

$$b^{xb^2} = b^{b^x}$$

soit $x = b^{x-2}$. Si $b = 1$, on a directement $x = 1$. Si $b \geqslant 2$, l'inégalité ne peut avoir lieu pour $x > 4$. Pour $x = 3$, on trouve $b = 3$ et pour $x = 4$, on trouve $b = 2$. Les solutions obtenues ainsi sont $(1,1)$, $(16,2)$ et $(27,3)$.

Si $a \leqslant b$, on a $a^{b^2} = b^a \leqslant b^b$ et donc $a^b \leqslant b$, ce qui est impossible si $a \geqslant 2$. On obtient ainsi la solution $(1,1)$ déjà trouvée.

Finalement les solutions sont $(1,1)$, $(16,2)$ et $(27,3)$.

Solution de l'exercice 195 : Soit (a,b) une solution de l'équation $a^2 + b^2 = n(ab+1)$ en entiers strictement positifs. On peut supposer a minimal parmi toutes les solutions en entiers strictement positifs. Alors en particulier, comme (b,a) est une telle solution, on a $a \leqslant b$.

D'autre part, $(na - b, a)$ est encore une solution, donc si $na - b > 0$, on doit avoir $na - b \geqslant a$. Mais alors en multipliant par b il vient :

$$ab \leqslant nab - b^2 = a^2 - n \leqslant ab - n$$

ce qui est absurde. Donc $na - b \leqslant 0$. Si l'inégalité est stricte, on a $b \geqslant na + 1 \geqslant n$ et donc :

$$n = a^2 + b^2 - nab = a^2 + b(b - na) \geqslant a^2 + n \cdot 1$$

ce qui est encore absurde. Il en résulte que $b - na = 0$, et donc $n = a^2$.

Finalement, si l'équation $a^2 + b^2 = n(ab+1)$ possède des solutions en entiers strictements positifs, n doit bien être un carré parfait.

Solution de l'exercice 196 : Si $a^2 + b^2 + c^2 = nabc$ avec $a \leqslant b \leqslant c$, alors c est l'une des racines du polynôme :

$$P(X) = X^2 - nabX + a^2 + b^2$$

La somme des racines étant nab, l'autre racine c' est également entière et positive (puisque le produit des racines l'est). D'autre part $P(b) = (3 - na)\,b^2 + a^2 - b^2$ qui est strictement négatif sauf si $na < 3$ ou si on a à la fois $na = 3$ et $a = b$. Le premier cas est exclu. En effet, pour $na \leqslant 2$, il vient :

$$a^2 + b^2 + c^2 - nabc \geqslant a^2 + (b - c)^2 > 0$$

Le second cas conduit aux solutions $n = 3$, $a = b = 1$ (donc $c = 1$ ou $c = 2$) et $n = 1$, $a = b = 3$ (et donc $c = 3$ ou $c = 6$), que l'on appelera *solutions minimales*.

si $n \geqslant 1$ et $n \geqslant 3$, puisque $P(b) < 0$, la seconde racine est strictement inférieure à b, et donc à c. Ainsi, on construit à partir d'une solution (a,b,c) non minimale une solution (a,b,c') plus petite. Le principe de descente infinie prouve que si $n \neq 1$ et $n \neq 3$, l'équation

n'admet aucune solution. Pour $n = 1$ ou $n = 3$, elle en admet une infinité qui s'obtiennent en remontant à partir des solutions minimales par la même transformation.

Solution de l'exercice 197 : **a)** Tous les entiers $n \geqslant 1$ conviennent, sauf $n = 2$. En effet, si $n = 1$, il suffit de choisir $a = b = 2$. Si $n \geqslant 3$, il suffit de choisir $a = (n-1)^{n-1}$ et $b = (n-1)^n$.

Prouvons désormais que $n = 2$ ne convient pas. Par l'absurde, supposons qu'il existe des entiers $a, b \geqslant 2$ tels que

$$(a^a)^2 = b^b \tag{10}$$

Une telle relation montre que tout nombre premier qui divise a divise également b. On peut aussi noter que si $b \leqslant a$ alors $b^b \leqslant a^a < (a^a)^2$, et que si $b \geqslant 2a$ alors $b^b \geqslant (2a)^{2a} = 2^{2a}(a^a)^2 > (a^a)^2$. Par suite, on doit avoir $a < b < 2a$.

Soit donc p un nombre premier qui divise a (et donc b). On note α (resp. β) l'exposant de p dans la décomposition de a (resp. de b) en facteurs premiers. La relation (10) conduit alors à $2a\alpha = b\beta$, c'est-à-dire $\alpha/\beta = b/2a < 1$, et donc $\alpha < \beta$.

Par suite, tout nombre premier qui divise a divise également b et ce, selon une puissance supérieure. Cela entraine que b est un multiple de a ce qui est impossible puisque $a < b < 2a$: contradiction !

b) On a déjà la solution évidente $(1, 1)$. Supposons maintenant que $a, b \geqslant 2$ soient des entiers tels que

$$(a^a)^5 = b^b \tag{11}$$

La démarche du a) s'adapte en tout point pour prouver que $a < b < 5a$ et que a divise b. Par suite, $b = ka$ où $k \in \{2, 3, 4\}$, et (11) s'écrit $a^{5a} = (ka)^{ka}$, c'est-à-dire $a^{5-k} = k^k$. Pour $k = 2$, cela conduit à $a^3 = 4$, ce qui est impossible. Pour $k = 3$, il vient $a^2 = 27$, ce qui est toujours impossible. Et si $k = 4$, on obtient $a = 4^4$ puis $b = 4^5$, et on vérifie qu'ils forment effectivement une solution de (11).

Finalement, les solutions sont $(1, 1)$ et $(4^4, 4^5)$.

Solution de l'exercice 198 : Posons $x = zc$ et $y = zb$ où b et c sont des entiers premiers entre eux. L'équation devient :

$$c + zb^2 + z^2 = z^2cb$$

On en déduit que z divise c et donc $c = za$ pour un certain entier a. L'équation se transforme à nouveau $a + b^2 + z = z^2ab$, c'est-à-dire :

$$a = \frac{b^2 + z}{z^2b - 1}$$

puis :

$$z^2a = b + \frac{b + z^3}{z^2b - 1}$$

Le terme $\frac{b+z^3}{z^2b-1}$ doit donc être un entier strictement positif, (donc supérieur ou égal à 1), et donc $b \leqslant \frac{z^2-z+1}{z-1}$. Ce majorant est inférieur strictement à $z+1$ dès que $z \geqslant 3$. Ainsi, si $z \geqslant 3$, on récupère $b \leqslant z$ et donc $a \leqslant \frac{z^2+z}{z^2-1} < 2$. Par suite $a = 1$ et l'équation devient :

$$1 + b^2 + z = z^2b$$

C'est une équation du second degré en b dont le discriminant est $z^4 - 4z - 4$. Il ne peut être un carré puisqu'il est strictement compris entre $(z^2-1)^2$ et z^4. On n'a donc aucune solution dans ce cas.

Il ne reste plus que les cas $z = 1$ et $z = 2$. Pour $z = 1$, on a :

$$a = \frac{b^2+1}{b-1} = b + 1 + \frac{2}{b-1}$$

donc $b = 2$ ou $b = 3$. On obtient alors deux solutions : $(x, y) = (5, 2)$ ou $(x, y) = (5, 3)$. Si $z = 2$, on écrit :

$$16a = \frac{16b^2+32}{4b-1} = 4b + 1 + \frac{33}{4b-1}$$

donc $b = 1$ ou $b = 3$. On obtient encore deux solutions : $(x, y) = (4, 2)$ ou $(x, y) = (4, 6)$.

Les solutions sont $(5, 2)$, $(5, 3)$, $(4, 2)$, $(4, 6)$.

Solution de l'exercice 199 : **a)** On suit la méthode de descente de Fermat. Donnons-nous des entiers strictement positifs x, y et z tels que $x^2 + y^2 = z^2$ et $\frac{xy}{2}$ soit un carré. On peut supposer x, y et z premiers entre eux, quitte à diviser par leur PGCD, ce qui fournit une solution plus petite. Dans ce cas, ils sont premiers entre eux deux à deux.

Quitte à échanger x et y, on peut écrire :

$$x = u^2 - v^2 \quad ; \quad y = 2uv \quad ; \quad z = u^2 + v^2$$

où u et v sont strictement positifs et premiers entre eux de parité contraire. L'aire du triangle est alors $uv(u-v)(u+v)$. Comme u et v sont de parité contraire, $u+v$ et $u-v$ sont impairs et donc premiers entre eux. Ainsi les quatre facteurs du produit sont premiers entre eux et donc chacun un carré. Il existe des entiers a, b et des entiers impairs c et d tels que :

$$u = a^2 \quad ; \quad v = b^2 \quad ; \quad u + v = c^2 \quad ; \quad u - v = d^2$$

On a $2b^2 = c^2 - d^2 \equiv 0 \pmod 4$ donc b est pair. On pose $b = 2b'$ d'où :

$$\left(\frac{c+d}{2}\right)\left(\frac{c-d}{2}\right) = 2b'^2$$

On a PGCD $(c+d, c-d) = 2$ (puisque ces deux nombres sont pairs) et donc un et un seul des deux facteurs précédents est pair.

Si c'est $\frac{c+d}{2}$. Alors :

$$\left(\frac{c+d}{4}\right)\left(\frac{c-d}{2}\right) = b'^2$$

Comme les deux facteurs sont premiers entre eux, il existe r et s tels que :

$$c + d = 4s^2 \quad ; \quad c - d = 2r^2$$

On vérifie que $a^2 = r^4 + 4s^4$, ce qui prouve que le triplet $(r^2, 2s^2, a)$ est une nouvelle solution dont on vérifie qu'elle est plus petite au sens où $a < z$.

Le principe de descente infinie permet de conclure qu'il n'y a pas de solution.

b) Soient x, y et z des entiers strictement positifs vérifiant :

$$x^4 - y^4 = z^2$$

On pose $X = x^4 - y^4$, $Y = 2x^2y^2$ et $Z = x^4 + y^4$. Alors X, Y et Z sont les côtés d'un triangle rectangle dont l'aire est un carré. D'après la question précédente n'est possible que si $X = 0$, c'est-à-dire $x = y$ et par le fait $z = 0$. Ceci n'est pas une solution acceptable.

Solution de l'exercice 200 : Soit p un diviseur premier de ℓ. Alors $\left(1+n^k\right)^p - 1$ divise $\left(1+n^k\right)^\ell - 1 = n^m$. Or, d'après la formule du binôme :

$$\left(1+n^k\right)^p - 1 = pn^k + \frac{1}{2}p\,(p-1)\,n^{2k} + Mn^{3k}$$

où M est un entier. Notons :

$$A = p + \frac{1}{2}p\,(p-1)\,n^k + Mn^{2k}$$

C'est un diviseur de n^m strictement supérieur à p. Si p ne divisait pas n, alors n serait premier avec A, ce qui contredit que A divise n^m. Donc p divise n et il divise aussi A. Le quotient $\frac{A}{p}$ est un entier strictement supérieur à 1 divisant n^m. On a en outre :

$$\frac{A}{p} = 1 + \frac{1}{2}\,(p-1)\,n^k + \frac{M}{p}n^{2k}$$

et chacun des trois termes est entier (pour le terme central, si $p = 2$, alors n est pair, et sinon $p - 1$ est pair). Le dernier terme est même multiple de n. Si $k > 1$ ou p est impair, n divise $\frac{1}{2}\,(p-1)\,n^k$, et donc n est premier avec $\frac{A}{p}$, ce qui contredit le fait que $\frac{A}{p}$ soit un diviseur de n^m.

Donc $k = 1$ et $p = 2$. Et donc $\ell = 2^s$ pour un certain entier $s \geqslant 1$. L'équation se réécrit :

$$n^m = (1+n)^\ell - 1 = n\ell + n^2M'$$

pour un certain entier $M' > 0$. On en déduit que $m \geqslant 2$ puis que n divise ℓ. Ainsi n est aussi une puissance de 2 : $n = 2^t$ pour un certain entier t.

On remarque que :

$$\begin{aligned} X^{2^s} - 1 &= \left(X^{2^{s-1}}+1\right)\left(X^{2^{s-1}}-1\right) \\ &= \left(X^{2^{s-1}}+1\right)\left(X^{2^{s-2}}+1\right)\left(X^{2^{s-2}}-1\right) \\ &\ \vdots \\ &= \left(X^{2^{s-1}}+1\right)\left(X^{2^{s-2}}+1\right)\cdots(X+1)\,(X-1) \end{aligned}$$

En l'appliquant à $X = 1 + n$, on obtient :

$$2^{tm} = n\left((1+n)^{2^{s-1}}+1\right)\left((1+n)^{2^{s-2}}+1\right)\cdots(n+2)$$

Ainsi n et $n + 2$ sont tous les deux des puissances de 2, ce qui n'est possible que si $n = 2$. Le facteur $(1+n)^2 + 1$ vaut alors 10 qui n'est pas une puissance de 2. Donc $s = 1$ et $n = 2$. Il s'ensuit $m = 3$.

Finalement la seule solution est $m = 3$, $n = 2$, $k = 1$ et $\ell = 2$.